ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ALLEN & GLEDSHILL LLP
BONELLIEREDE
BURGES SALMON LLP
BUZKO LEGAL
CMS REICH-ROHRWIG HAINZ RECHTSANWÄLTE GMBH
COLLAS CRILL
DLA PIPER UK LLP
GILBERT + TOBIN
HAMMAD AND AL-MEHDAZ
HENRY YU & ASSOCIATES, IN ASSOCIATION WITH L & Y LAW OFFICE
HOGAN LOVELLS
HUNTON ANDREWS KURTH LLP
KIM & CHANG
LEE AND LI, ATTORNEYS-AT-LAW
LOYENS & LOEFF
MORI HAMADA & MATSUMOTO
NIEDERER KRAUT FREY
NOERR LLP
SK CHAMBERS
SRP-LEGAL
TOZZINIFREIRE ADVOGADOS
URÍA MENÉNDEZ
VIEIRA DE ALMEIDA

© 2020 Law Business Research Ltd
## CONTENTS

PREFACE ............................................................................................................................................. vii  
*Thomas A Frick*

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Country</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AUSTRALIA</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>by Peter Reeves</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>AUSTRIA</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>by Stefan Paulmayer</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>BELGIUM</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>by Pierre E Berger and Marc Van de Looverbosch</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>BRAZIL</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>by Alexei Bonamin, Marcela Waksman Ejnisman, Carla do Couto Hella Battilana, Marcus Fonseca, Felipe Borges Lacerda Loiola, Natasha Wiedmann and Victor Cabral Fonseca</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>BRITISH VIRGIN ISLANDS</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>by Ian Montgomery</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>CAYMAN ISLANDS</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>by Alan de Saram, Natalie Bell, Aoife Madden, Laura Smalley and Dawn Major</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>GERMANY</td>
<td>73</td>
</tr>
<tr>
<td></td>
<td>by Jens H Kunz</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>GUERNSEY</td>
<td>94</td>
</tr>
<tr>
<td></td>
<td>by Wayne Atkinson</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>HONG KONG</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>by Yu Pui Hang (Henry Yu)</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>ITALY</td>
<td>117</td>
</tr>
<tr>
<td></td>
<td>by Giuseppe Rumi, Federico Vezzani and Tommaso Faelli</td>
<td></td>
</tr>
</tbody>
</table>

© 2020 Law Business Research Ltd
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Country</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>JAPAN</td>
<td>Atsushi Okada, Takane Hori and Takahiro Iijima</td>
<td>134</td>
</tr>
<tr>
<td>12</td>
<td>JERSEY</td>
<td>Dilmun Leach</td>
<td>148</td>
</tr>
<tr>
<td>13</td>
<td>LUXEMBOURG</td>
<td>Anne-Marie Nicolas, Álvaro Garrido Mesa and Sandy Brumberg</td>
<td>159</td>
</tr>
<tr>
<td>14</td>
<td>MALAYSIA</td>
<td>Shanthi Kandiah</td>
<td>174</td>
</tr>
<tr>
<td>15</td>
<td>MEXICO</td>
<td>Federico de Noriega Olea and Juan Enrique Lizardi Becerra</td>
<td>184</td>
</tr>
<tr>
<td>16</td>
<td>NETHERLANDS</td>
<td>Martijn Schoonewille, Wendy Pronk, Marije Louise, Mariska Kool and Pepijn Pinkse</td>
<td>194</td>
</tr>
<tr>
<td>17</td>
<td>PORTUGAL</td>
<td>Tiago Correia Moreira, Helena Correia Mendonça, Conceição Gamito, José Miguel Carracho and Francisca César Machado</td>
<td>205</td>
</tr>
<tr>
<td>18</td>
<td>RUSSIA</td>
<td>Roman Buzko</td>
<td>220</td>
</tr>
<tr>
<td>19</td>
<td>SAUDI ARABIA</td>
<td>Suhaib Adli Hammad</td>
<td>230</td>
</tr>
<tr>
<td>20</td>
<td>SINGAPORE</td>
<td>Adrian Ang V-Meng and Alexander Yap Wei-Ming</td>
<td>239</td>
</tr>
<tr>
<td>21</td>
<td>SOUTH KOREA</td>
<td>Jung Min Lee, Joon Young Kim and Samuel Yim</td>
<td>247</td>
</tr>
<tr>
<td>22</td>
<td>SPAIN</td>
<td>Leticia López-Lapuente and Isabel Aguilar Alonso</td>
<td>261</td>
</tr>
<tr>
<td>23</td>
<td>SWITZERLAND</td>
<td>Thomas A Frick</td>
<td>272</td>
</tr>
</tbody>
</table>
Chapter 24  TAIWAN ............................................................................................................................ 284
Abe T S Sung and Eddie Hsiung

Chapter 25  TURKEY .......................................................................................................................... 295
Cigdem Ayozger Ongun, Filiz Piyal and Deniz Erkan

Chapter 26  UNITED KINGDOM ........................................................................................................ 303
Gareth Malna and Sarah Kenshall

Chapter 27  UNITED STATES ............................................................................................................ 315
Erin Fonte, Scott Kimpel, Carleton Goss, Brenna McGee and Patrick Boot

Appendix 1  ABOUT THE AUTHORS .............................................................................................. 333
Appendix 2  CONTRIBUTORS’ CONTACT DETAILS ........................................................................... 357
This is already the third edition of The Financial Technology Law Review. If anything, concerns about certain aspects of the new developments that blockchain, Big Data and artificial intelligence (AI) trigger in the finance sector have increased since the first edition. In particular, developments such as the announcement of Facebook's Libra project or certain aspects of AI continue to worry regulators. However, the fact that certain high-profile projects receive critical attention should not obscure the fact that fintech has moved to become quite an established part of the financial ecosystem. Both financial market participants and their legal advisers already have considerable experience in implementing fintech projects by now. Not only are a significant number of start-ups presenting new fintech projects, but more and more established market participants such as banks, insurance companies and exchanges are setting up fintech labs and experiments, in part also implementing fintech projects and products.

After the initial hype, the number of active cryptocurrencies imitating Bitcoin and Ethereum have diminished considerably. Other developments continue, in particular, exploring the new ways of organising business that stablecoins and security tokens may offer. The use of Big Data and AI, closely interlinked, is starting to move from exploratory projects to the application stage. After the widespread scepticism that was referred to in the preface to the second edition of this book, market participants are again starting to see the opportunities these new technologies offer, even if not all projects will lead to a disruption of the industry. A new realism and a greater awareness of the opportunities and risks involved seem to have arrived. It may be that the current corona-virus crisis will even encourage this development, as many enterprises are in the process of furthering the digitalisation of their business.

Though the regulators’ initial surprise about the sheer dynamism of these projects has ebbed, there are numerous initiatives both on the national and on the international level to provide sandboxes for fintech start-ups and to regulate fintech. Implementation of an effective anti-money laundering system continues to concern not only the regulators, but also banks and other financial market participants. Unless the industry can be certain that participating in the crypto-economy will not lead to increased anti-money laundering risks, established financial players remain cautious. However, even the Bank for International Settlement, after highly critical initial statements, initiated a discussion paper on designing prudential treatment for cryptoassets in December 2019, and the FATF published guidance on virtual assets in June 2019.

The national solutions chosen vary considerably between jurisdictions, not only owing to different regulatory cultures, but also to differences in the treatment under contract and tort law of some of the new issues arising. In the absence of a harmonised international regime, the structured collection of overviews on certain aspects of fintech law and regulation
this book continues to be valuable not only for the international practitioner, but also for anyone looking for inspiration on how to deal with hitherto unaddressed and unthought-of issues under the national law of any country.

The authors of this publication are from the most widely respected law firms in their jurisdictions. They each have a proven record of experience in the field of fintech; they know both the law and how it is applied. We hope that you will find their experience invaluable and enlightening when dealing with the varied issues fintech raises in the legal and regulatory field.

The emphasis of this book is on the law and practice of each of the jurisdictions, but discussion of emerging or unsettled issues has been provided where appropriate. The views expressed are those of the authors and not of their firms, nor of the editor or the publisher. In a fast-changing environment, every effort has been made to provide the latest intelligence on the current status of the law.

Thomas A Frick
Niederer Kraft Frey
Zurich
March 2020
Chapter 1

AUSTRALIA

Peter Reeves

I OVERVIEW

The Australian financial services sector has continued to give significant attention to the fintech industry, with a range of regulatory and legislative developments facilitating innovations and new businesses entering the market. Australian regulators and policy-makers have sought to improve their understanding of, and engagement with, fintech businesses by regularly consulting with industry on proposed regulatory changes and entering into international cooperation and information sharing agreements.

Australian regulators have been receptive to supporting the entrance of fintechs, streamlining access and offering informal guidance to enhance regulatory understanding. Both the Australian Securities and Investments Commission (ASIC) and the Australian Transaction Reports and Analysis Centre (AUSTRAC) have established innovation hubs to assist start-ups in navigating the Australian regulatory regime. AUSTRAC's Fintel Alliance also has an innovation hub targeted at combating money laundering and terrorism financing, and improving the fintech sector's relationship with government and regulators.

ASIC has entered into a number of cooperation agreements with overseas regulators that aim to further understand the approach of fintech businesses in other jurisdictions, in an attempt to better align the treatment of these businesses across jurisdictions. These cross-border agreements facilitate the referral and sharing of information on fintech market trends, encourage referrals of fintech companies and share insights from proofs of concepts and innovation competitions. A number of these agreements aim to further understand the approach to regulation of fintech businesses in other jurisdictions in an attempt to better align the treatment of these businesses across jurisdictions. ASIC has committed to supporting financial innovation in the interests of consumers by joining the Global Financial Innovation Network, which launched in January 2019 and currently has 50 member organisations.

In December 2016, ASIC made certain class orders establishing a fintech licensing exemption and released regulatory guidance detailing its regulatory sandbox for fintech businesses to test certain financial services, financial products and credit activities without holding an Australian financial services licence (AFSL) or Australian credit licence (ACL). There are strict eligibility requirements for both the type of businesses that can enter the regulatory sandbox and the products and services that qualify for the licensing exemption. Once a fintech business accesses the regulatory sandbox, there are restrictions on how many persons can be provided with a financial product or service and caps on the value of the financial products or services that can be provided.

1 Peter Reeves is a partner at Gilbert + Tobin.
Investments in fintechs can, among other structures, be made through Australian incorporated limited partnerships called ‘early-stage venture capital limited partnerships’ and ‘venture capital limited partnerships’. Such investments may receive favourable tax treatment. Depending on the investment vehicle, benefits can include tax exemptions for resident and non-resident investors on revenue and capital gains on a disposal of the investment, plus a 10 per cent non-refundable tax offset available for new capital invested and the carried interest of fund managers being treated on capital account.

A programme known as the R&D Tax Incentive is available for entities incurring eligible expenditure on R&D activities, which includes certain software R&D activities commonly conducted by fintechs. Claimants under the R&D Tax Incentive may be eligible for one of the following incentives:

- **Small businesses** (less than A$20 million aggregated turnover) not controlled by exempt entities: a 43.5 per cent refundable tax offset; and
- **Other businesses** (over A$20 million aggregated turnover or controlled by exempt entities): a 38.5 per cent non-refundable tax offset for eligible expenditure below A$100 million and 30 per cent for eligible expenditure over A$100 million.

Significant changes to the R&D Tax Incentive are expected subject to the passing of the Treasury Laws Amendment (Research and Development Tax Incentive) Bill 2019. Among the changes is the introduction of an ‘incremental intensity threshold’ which increases or decreases a business’ non-refundable tax offset based on how much the company spends on R&D. These changes are expected to apply retrospectively to income years commencing on or after 1 July 2019.

## II REGULATION

### i Licensing and marketing

**Licensing and marketing**

In Australia, the regulatory framework applicable to fintech companies broadly includes banking regulation, financial services licensing, consumer credit licensing, registration and disclosure requirements, consumer law obligations, data and privacy regulation, payment regulation and anti-money laundering and counter-terrorism financing requirements.

Fintech businesses carrying on a financial services business in Australia must hold an AFSL or be exempt from the requirement to be licensed. The Corporations Act 2001 (Cth) (the Corporations Act), which is administered by ASIC, broadly defines a financial service to include the provision of financial product advice, dealing in financial products (as principal or agent), making a market for financial products, operating registered schemes and providing custodial or depository services. A financial product is a facility through which, or through the acquisition of which, a person makes a financial investment, manages a financial risk or makes a non-cash payment (NCP).

These definitions are broad and will generally capture any deposit taking business, investment or wealth management business, payment service (e.g., NCP), advisory business (including robo-advice), trading platform, crowdfunding platform and other fintech offerings. Certain financial product advice will also require an AFSL, including the provision of automated digital advice so long as it can reasonably be regarded as intending to influence a client to make decisions in relation to financial products or services.
The ACL regime applies to fintechs who engage in consumer credit activities in Australia, for example, providing credit under a credit contract or consumer lease. Any person engaging in consumer credit activities must hold an ACL, or otherwise be exempt from the requirement. Consumer credit activity is regulated by ASIC under the National Consumer Credit Protection Act 2009 (Cth) (the National Credit Act) and associated regulations. In addition to holding an AFSL, fintechs that provide marketplace lending products and related services, such as peer-to-peer lending and crowd-lending platforms, will generally constitute consumer credit activities and trigger the requirement to hold an ACL.

The provision of credit information services in Australia is subject to the Privacy Act 1988 (Cth) (the Privacy Act), which provides that only credit reporting agencies (i.e., corporations carrying on a credit-reporting business) are authorised to collect personal information, collate it in credit information files and disclose it to credit providers. Credit reporting agencies must comply with obligations with regard to use, collection and disclosure of credit information.

Fintech businesses may also need to hold an Australian market licence where they operate a facility through which offers to buy and sell financial products are regularly made and accepted (e.g., an exchange). If an entity operates a clearing and settlement mechanism that enables parties transacting in financial products to meet obligations to each other, the entity must hold a clearing and settlement facility licence or be otherwise exempt.

Most financial services businesses will have obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (the AML/CTF Act) and Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (the AML/CTF Rules). Anti-money laundering and counter-terrorism financing (AML/CTF) laws apply to entities that provide ‘designated services’ with an Australian connection. Generally, the AML/CTF Act applies to any entity that engages in financial services, remittance or credit (consumer or business) activities in Australia. In 2018, the AML/CTF Act was amended to capture entities that provide digital currency exchange services. Obligations include enrolment (and, in some circumstances, registration) with AUSTRAC, conducting customer due diligence prior to providing any designated services and adopting and maintaining an AML/CTF programme.

Any entity that conducts any ‘banking business’, such as taking deposits (other than as partial payment for identified goods or services) or making advances of money, or provides a purchased payment facility, must be licensed as an authorised deposit-taking institution (ADI). The Australian Prudential Regulation Authority (APRA) is responsible for the authorisation process and granting of ADI licences (as well as ongoing prudential supervision). In 2018, APRA released the restricted ADI framework, which is designed to assist new businesses wishing to enter the banking industry. Under this regime, entities can conduct a limited range of business activities for two years while they build their capabilities and resources. After such time, they must either transition to a full ADI licence and operate without restriction, or exit the industry. As of January 2020, there is one restricted ADI on APRA’s register but several restricted ADIs have transitioned to holding full ADI status since 2018. Being an ADI allows such entities to operate as ADIs without restrictions under the Banking Act 1959 (Cth) (Banking Act).

Cloud computing is permitted for financial services companies. From a risk and compliance perspective, the same requirements, tests and expectations apply to cloud computing as would apply to other areas of a financial services business. ASIC has released
regulatory guidance indicating its expectations for licensees’ cloud computing security arrangements as well as frameworks that identify relevant compliance measures that should be put in place.

Marketing financial services may itself constitute a financial service requiring an AFSL. If financial services will be provided to retail clients, a financial services guide must first be provided, setting out prescribed information, including the provider’s fee structure, to assist a client to decide whether to obtain financial services from the provider. Retail clients wishing to buy a financial product must receive a disclosure document in the form of a product disclosure statement (PDS), which must contain sufficient information such that the retail client can make an informed decision about their purchase. Broadly, a PDS must contain the risks and benefits of acquiring the financial product, the significant characteristics of the financial product and the fees payable in respect of the financial product.

Fintech businesses are also subject to the Australian Consumer Law, which is administered by the Australian Competition and Consumer Commission (ACCC). Broadly, this includes prohibitions on misleading and deceptive conduct, false or misleading representations, unconscionable conduct and unfair contract terms. While the Australian Consumer Law does not apply to financial products or services, many of these protections are enforced by ASIC, either through mirrored provisions in the Australian Securities and Investments Commission Act 2001 (Cth) (the ASIC Act) or through delegated powers.

ii Cross-border issues

Passporting

It has been common in Australia for foreign financial services providers (FFSPs) to provide financial services to wholesale clients by relying on ASIC’s ‘passport’ exemption from the requirement to hold an AFSL. Before providing financial services, FFSPs must disclose to clients that they are exempt from holding an AFSL and that they are regulated and authorised to provide those financial services by the laws of a foreign jurisdiction.

FFSPs that are currently provided with passport relief through class orders in Australia include the United Kingdom, the United States Securities and Exchange Commission, Commodity Futures Trading Commission, Federal Reserve and Office of the Comptroller of the Currency-regulated financial services providers, the Singapore Monetary Authority of Singapore, the Hong Kong Securities and Futures Commission, the German BaFin and Luxembourg regulated financial service providers.

However, ASIC has announced that it will be proceeding with a proposal to repeal the passport and limited connection relief outlined above and will implement a new regime that will require FFSPs to apply for a foreign AFSL (i.e., a modified form of an AFSL for FFSPs). Passport relief will cease to be available from 31 March 2020. FFSPs relying on passport relief will have 24 months (until 31 March 2022) to transition to a foreign AFSL or satisfy licensing requirements in some other way. FFSPs relying on limited connection relief will have until 30 September 2020 to transition to a foreign AFSL or satisfy licensing requirements in an other way.

In June 2018, the Australian government passed the Corporations Amendment (Asia Region Funds Passport) Act 2018 (Cth), which incorporates the Asia Region Funds Passport (Passport) into the Corporations Act. The Passport is a region-wide initiative to facilitate the offer of interests in certain collective investment schemes established in Passport member economies to investors in other Passport member economies. It aims to provide Australian fund managers with greater access to economies in the Asia-Pacific by reducing
existing regulatory hurdles. Australia, Japan, Korea, New Zealand and Thailand are all signatories to the Passport’s Memorandum of Cooperation. Following its official launch on 1 February 2019, the Passport now has the first application for registration as a passport fund under review with the New Zealand Financial Markets Authority. Japan, Thailand and Australia are also available to receive registration applications from local prospective funds and entry applications from foreign Passport funds.

The Australian Treasury has also completed three tranches of consultation in relation to the Corporate Collective Investment Vehicle scheme (CCIV). The CCIV will be a new type of investment vehicle that aims to expand the range of collective investment schemes offered in Australia and will enhance the competitiveness of funds by improving access to overseas markets. The CCIV regime is intended to complement the Passport, which will allow Australian fund managers to pursue overseas investment opportunities through a company structure. The CCIV will be implemented through the Treasury Laws Amendment (Collective Investment Vehicle) Bill 2017 and an additional Bill to enact amendments to other legislation, including the Corporations Act.

Although there are concerns that the reforms will add extra complexity to existing corporate, partnership and tax laws, the enactment of the Passport and the CCIV has the potential to open significant financing opportunities for fintech businesses.

**Australian presence**

Foreign companies, including fintechs, wishing to access Australian customers must overcome a number of regulatory hurdles. These include registering with ASIC in order to carry on a business in Australia which is generally satisfied by either establishing a local presence (i.e., registering a branch office) or incorporating an Australian subsidiary. Generally, the greater the level of system, repetition or continuity associated with an entity’s business activities in Australia, the greater the likelihood registration will be required.

**Marketing foreign financial services**

Generally, an offshore provider can address requests for information, pitch and issue products to an Australian customer if the customer makes the first approach (i.e., there has been no conduct designed to induce the investor, or that could have been taken to have that effect) and the service is provided from outside Australia.

If the unsolicited approach relates to credit activities that are regulated under the National Credit Act, the provider is required to hold an ACL irrespective of the unsolicited approach.

**Foreign exchange and currency-control restrictions**

Australia does not have foreign exchange or currency-control restrictions on the flow of currency into or out of the country. However, there are cash-reporting obligations to AUSTRAC. To control tax evasion, money laundering and organised crime, AUSTRAC must receive reports of transfers of A$10,000 or more (or the foreign currency equivalent) and reports of suspicious transactions from reporting entities such as banks, building societies and credit unions. Unless an exemption applies, reporting entities must also submit an AML/CTF compliance report to AUSTRAC, which collects information about the appropriateness of a reporting entity’s money laundering and terrorism financing risk assessments and of its AML/CTF compliance programme.
III DIGITAL IDENTITY AND ONBOARDING

There is no generally recognised digital identity in Australia. However, following a request for information from the industry on its alpha design phase, the Australian federal government’s Digital Transformation Agency (DTA) is currently in the beta stage of developing a centralised digital identity platform. The national overarching digital identity technology called ‘GovPass’ is divided into four components; the Trusted Digital Identity Framework (TDIF), the exchange gateway, the digital identity services and the services providers. The TDIF governs the platform Govpass and allows people to choose their identity provider and access a range of government services, with an opportunity for future integration with the private sector.

Currently, the GovPass digital identity has only been used for a limited number of government services. However, this is set to change in March 2020 with the Australian government’s identity provider, ‘myGovID’, set to replace AUSKey, a secure login that identifies individuals using participating government services on behalf of a business.

There is also another digital identity service in use in Australia called ‘Digital iD’, which was launched in mid-2017 by Australia Post. The smartphone-based platform is being used by Australia Post and certain early adopter organisations. The DTA has partnered with Australia Post to work towards the incorporation of Australia Post’s Digital iD as one of the identity providers under the broader GovPass project.

Financial services providers are able to carry out fully digitised onboarding of clients, subject to know your customer (KYC) and AML/CTF obligations being complied with. Under the AML/CTF Rules, electronic verification of client information and data may be undertaken with or without hard-copy documentation. Financial services providers may use safe harbour documentation-based or electronic-based procedures to verify individuals where the reporting entity determines that the relationship with the customer is of medium or lower money laundering or terrorism risk.

Entities required to report to AUSTRAC who want to use electronic verification must verify the client’s name and residential address using reliable and independent electronic data from at least two separate data sources and either the client’s date of birth or residential address, or the client’s transaction history for at least the past three years. Financial services providers must also receive express and informed client consent to use electronic verification. Reporting entities are required to retain information about verification requests and assessments for the life of the client relationship and for seven years from the date of the request after ceasing to provide the designated services to a client.

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i Digital marketplaces and cryptoassets

At the time of writing, there are no special rules in Australia that have been implemented to specifically regulate digital markets or cryptoassets. Generally, cryptoassets are regulated under existing regulatory frameworks. If a digital marketplace deals in cryptoassets that are financial products, then the platform is operating a market and a range of Australian laws apply, including the requirement to hold an Australian market licence and an AFSL. See Section II for further detail.
ii Collective investment schemes

Collective investment schemes in Australia are generally referred to as managed investment schemes, which can be contract-based schemes, unincorporated vehicles (typically structured as unit trusts or unincorporated limited partnerships) or bodies corporate (which are incorporated and typically structured as companies or incorporated limited partnerships).

Depending on the structure, a platform or scheme operated by a fintech company may fall within the scope of the Australian collective investment scheme regulations. They may also be subject to AFSL, ACL, consumer law and financial services laws relating to consumer protection under the ASIC Act.

iii Crowdfunding

In September 2017, a regulatory framework was introduced for crowd-sourced equity funding (CSF) by public companies from retail investors. The CSF regime enables companies to raise funds from large pools of investors by utilising a licensed CSF platform instead of listing on a stock exchange. While the regime reduces the regulatory barriers to investing in small and start-up businesses, the framework also created certain licensing and disclosure obligations for CSF intermediaries (i.e., persons listing CSF offers for public companies). ASIC has released Regulatory Guides 261 and 262 to assist companies seeking to raise funds through CSF and intermediaries seeking to provide CSF services, respectively.

The government passed the Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Bill 2017 (Cth), extending the CSF regime to proprietary companies. While there are a range of reporting requirements imposed on proprietary companies engaging in crowdfunding, there are also a number of concessions made with respect to restrictions that would otherwise apply to their fundraising activities.

Notably, the government has previously indicated its intention to consult on the extension of the existing CSF regime to debt funding. Although debt financing is less common than equity raising for fintech businesses in Australia, businesses can approach institutions, suppliers and finance companies in relation to debt finance.

iv Marketplace lending

Providers of marketplace lending products, including those peer-to-peer lending services, are generally structured such that they need to hold an AFSL and comply with the relevant requirements outlined in the Corporations Act including appropriate disclosure and resourcing requirements.

Where the loans are consumer loans (e.g., loans to individuals for domestic, personal or household purposes), the provider will also need to hold an ACL and comply with requirements in the National Credit Act and the National Credit Code. Similarly, all loans (including loans for a business purpose that are not regulated under the National Credit Act) are subject to consumer protections provisions in the ASIC Act, including prohibitions on misleading or deceptive representations. Peer-to-peer lenders are sometimes structured as managed investment schemes, which must be registered with ASIC if the investment is offered to retail investors.

There are generally no restrictions on secondary markets for trading loans; however, such activities may trigger licensing obligations for the provider of the market, market maker and market participants.
v Payment services
Payment services may be regulated as financial services because this concept captures services relating to deposit-taking facilities made available by an ADI in the course of carrying on a banking business or a facility through which a person makes a NCP.

If an entity facilitates an NCP, the service provider must hold an AFSL or be exempt from the requirement to do so. ASIC has outlined a number of exceptions including general exemptions in relation to specific NCP products such as gift vouchers and loyalty schemes.

As discussed in Section II, any entity that conducts banking business must also be licensed as an ADI.

vi Data sharing
In Australia there is no requirement to make client data accessible to third parties; however, this is often necessary for lenders and credit reporting agencies who must comply with obligations with regard to use, collection and disclosure of credit information (see Section II).

The Privacy Act includes 13 Australian Privacy Principles (APP) which impose obligations on the collection, use, disclosure and destruction of personal information.

In Australia significant changes are proposed in relation to how customer data is shared with third parties across every sector of the Australian economy. In 2018, the Notifiable Data Breaches (NDB) scheme was introduced requiring entities regulated under the Privacy Act to notify any affected individuals and the Office of the Australian Information Commissioner in the event of a data breach (i.e., the unauthorised access to or disclosure of information) that is likely to result in serious harm to those individuals. The NDB scheme applies to agencies and organisations that the Privacy Act requires to take steps to secure certain categories of personal information.

The Australian government will be implementing the national consumer data right (CDR) framework, which will give customers a right to share their data with accredited services providers (including banks, comparison services, fintechs or third parties). The CDR framework will first be applied to the banking sector under the Open Banking regime by which consumers can exercise greater access and control over their banking data. In September 2019, 10 companies were selected to participate in a trial, with the Open Banking regime slated to formally commence in July 2020.

The European Union (EU) General Data Protection Regulation also has a broad extraterritorial reach and may significantly impact the data handling practices of data for Australian businesses providing goods and services in the EU.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS
i Blockchain
There are currently no specific regulations dealing with blockchain technology in Australia. However, in March 2017, ASIC released guidance outlining its approach to the regulatory issues that may arise through the implementation of blockchain technology and distributed ledger technology (DLT) solutions in fintech businesses more generally. ASIC reaffirmed their ‘technology neutral’ stance in applying the financial services regime and the notion that businesses considering operating market infrastructure or providing financial or consumer credit services using DLT will still be subject to the compliance requirements that currently exist under the applicable regulation.

© 2020 Law Business Research Ltd
ii Cryptocurrencies

In May 2018, ASIC updated its guidance on initial coin offerings (ICOs) to include clarification on the corporate and consumer law consequences that may arise in an ICO context, including the prohibition on misleading and deceptive conduct. While tokens may be offered to Australian residents from abroad, token offerors should note that the Australian Consumer Law on misleading and deceptive conduct will still apply.

ASIC's regulatory guidance informs businesses of their approach to the legal status of coins or tokens offered through ICOs in Australia. The legal status of such coins is dependent on how the ICO is structured and the rights attached to the coins. Depending on the circumstances, ICOs may be considered to be managed investment schemes, an offer of securities or fall into a category of more generally defined financial products all of which are sometimes referred to as an STO or security token offering. In these instances, entities offering such coins will need to comply with financial services regulatory requirements under the Corporations Act. An entity that facilitates payments by cryptocurrencies may also be required to hold an AFSL. If an ICO constitutes an offer of financial products, this will impact the marketing of the ICO and its disclosure obligations. Cryptocurrencies are also subject to the general consumer protection provisions, prohibiting false or misleading representations and unconscionable conduct.

Under the AML/CTF Act, the Australian government has brought cryptocurrencies and tokens within the scope of Australia’s anti-money laundering regime. The regime is focused on the point of intersection between cryptocurrencies and the regulated financial sector, namely digital currency exchanges, and came into force on 3 April 2018. Digital currency exchange providers are required to register with AUSTRAC in order to operate. Registered exchanges are required to implement KYC processes to adequately verify the identity of their customers, with ongoing obligations to monitor and report suspicious and large transactions. Exchanges are required to keep certain records relating to customer identification and transactions for up to seven years. Operating a registrable digital currency exchange service without registering with AUSTRAC is an offence carrying a penalty of up to two years’ imprisonment or a fine of up to A$105,000, or both.

For income tax purposes, the Australian Taxation Office (ATO) currently views cryptocurrencies as neither money nor a foreign currency. Instead, each cryptocurrency is treated as a separate capital gains tax (CGT) asset. This means that gains made on the disposal of a cryptocurrency may be subject to income tax. In some instances where a cryptocurrency is held as an investment for at least 12 months, taxpayers may be entitled to a CGT discount to reduce the capital gain made on the disposal of the cryptocurrency. Also, certain capital gains or losses may be disregarded where there is a disposal of a cryptocurrency that is a personal use asset (i.e., an asset kept or used mainly to purchase items for personal use or consumption). The ATO's views on the income tax implications of transactions involving cryptocurrencies is in a state of flux due to the rapid evolution of both cryptocurrency technology and its application.

Effective from 1 July 2017, the Australian government amended the goods and services tax (GST) Act to the effect that the sale, including ICOs, or purchase of cryptocurrencies (namely those fulfilling the requirements for ‘digital currencies’ in the GST Act, such as Bitcoin, Ethereum, Litecoin, Dash, Monero, ZCash, Ripple and YbCoin) is not subject to GST. Instead, these sales and purchases will be input taxed such that no GST will be payable but entities registered for GST may be restricted from claiming input tax credits on the costs associated with the sale or purchase of cryptocurrencies. No GST will be payable
if the cryptocurrency is acquired by a non-resident for its overseas business because this will be a GST-free supply. The GST treatment is different still for businesses that receive cryptocurrency in return for their goods and services – in these circumstances, they will be subject to the normal GST rules. In other words, where taxable supplies of goods and services are made by businesses for which cryptocurrency is received as payment, GST will be imposed at the usual rate of 10 per cent on the taxable supply. This is because cryptocurrency is treated as a method of payment and the GST consequences of using it as payment are the same as the GST consequences of using money as payment.

iii Security tokens
As discussed in Section II, if a token falls within the definition of a financial product, the Australian laws relating to financial products will apply. Regardless of whether a token constitutes a financial product, ICOs and security token offerings will be subject to Australian consumer law restrictions and AML/CTF reporting requirements. There have been significant technological developments and sandbox experiments digitising security interests in a blockchain environment, but no corresponding legal reform to facilitate issuing or transferring legal title to such products on-chain. The numerous small-scale Australian and offshore blockchain-based bond issuances to date only mirror off-chain transactions on an on-chain ledger and do not provide for dealings in legal title or an on-chain payment rail that are impediments to widespread adoption.

VI OTHER NEW BUSINESS MODELS
i Smart contracts
Self-executing contracts or ‘smart contracts’ are permitted in Australia under the Electronic Transactions Act 1999 (Cth) (ETA) and the equivalent Australian state and territory legislation. The ETA provides a legal framework to enable electronic commerce to operate in the same way as paper-based transactions. Under the ETA, self-executing transactions are permitted in Australia, provided they meet all traditional elements of a legal contract: intention to create legally binding obligations, offer and acceptance, certainty and consideration.

Any attempt at an analysis of correction mechanisms, such as arbitration and mediation, in regard to this type of contract is challenging because there is little case law on smart contracts in Australia. Self-executing contracts may alter traditional dispute resolution in Australia based on the possibility of self-executing dispute resolution through online dispute resolution platforms.

ii Automated investments
Generally, fully automated investments are permitted in Australia on the condition that the automated service provider holds an AFSL, or is an authorised representative of a holder of an AFSL, with the requisite managed discretionary account (MDA) authorisation. Automated services providers and their retail clients are required to enter into individual MDA contracts to engage in this process. An MDA contract allows trades to be completed on a client’s behalf and includes the ability to automatically adjust the asset allocation of a client’s portfolio, without prior reference to the client for each individual transaction. Automated investment service providers must also comply with certain conduct and disclosure obligations applicable to providing the automated financial product service.
iii Artificial intelligence
At the time of writing, in Australia there are no special laws applicable to the use of artificial intelligence and machine learning. However, other general data protections including the Privacy Act and the NDB regime will apply. See Section IV(vi) for more detail.

iv Third-party websites
Third-party comparison websites that allow consumers to compare quotes on financial products must ensure they are providing accurate information and not misleading consumers, and may need to be licensed or be an authorised representative of an AFSL holder. ASIC has released guidance for operators of comparison websites, noting that generally operators should clearly disclose the basis of awards or ratings, disclose any links to the providers of products being compared including a warning if not all providers are being compared, clearly disclose advertisements and, where necessary, include a warning that the financial products compared do not compare all features that may be relevant for the consumer.

The ACCC, as Australia's competition and consumer law regulator, also has jurisdiction over comparison websites. The ACCC is primarily concerned with the way in which comparison websites drive competition and help consumers make informed decisions. Comparable to ASIC, the ACCC sets out guidance on how third-party comparison websites can facilitate honest comparisons of financial products and services, disclose commercial relationships between comparisons and financial product providers, and provide full disclosure of the financial products and providers that are being compared.

v Other new business models
In January 2019, the first Restricted ADI licensee was granted a full ADI licence allowing it to operate as an ADI without restrictions under the Banking Act. The licensee is a 'neobank', which is a wholly digital bank that intends to provide full banking services to customers via a solely mobile-based platform. The Restricted ADI licence which launched in 2018, is designed to assist new businesses to enter the banking industry and overcome the significant regulatory challenges faced when entering the market. There has been an increase in the number of digital-only banks and consumer support for the same, with two new neobanks launched in Australia and another neobank with an approved banking licence that is yet to be launched to the public.

There has also been a steady increase in the establishment of NCP platforms and solutions aimed at maximising cost and time efficiencies and improving customer experience. The New Payments Platform (NPP) was launched in Australia in February 2018 as the result of industry-wide collaboration between Australia's largest banks and financial institutions as well as Australia's central bank, the Reserve Bank of Australia. Over time, the NPP is expected to replace a significant portion of direct payments between consumers' bank accounts, particularly those that are time-critical or benefit from additional data capabilities.

Australia has also seen a proliferation in the use of blockchain technology and a growth of interest in the use of DLT by established businesses. Fintech businesses are gradually moving beyond the concept stage to formalising actual use cases in areas of managing supply chains, trading derivatives, managing and issuing assets, making cross-border payments and digital currency exchanges. The Australian Securities Exchange (ASX) is continuing with its plan to replace its core clearing and settlement process with a blockchain-based system. The ASX is currently in its consultation and development phase and has set a target go-live date of April 2021.
There have also been a number of private sector projects that have used blockchain to deliver services to consumers. Three of Australia’s four major banks have partnered with IBM and Scentre Group to establish an eight-week trial managing bank guarantees for retail property leases on blockchain, reducing the issuance period for a bank guarantee from up to a month to approximately the same day.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

The most appropriate forms of intellectual property (IP) protection in Australia for fintech business models and related software are patent and copyright.

Patent protection is available for certain types of innovations and inventions in Australia. A standard patent provides long-term protection and control over an invention, lasting for up to 20 years from the filing date. The requirements for a standard patent include the invention being new, involving an inventive step and being able to be made or used in an industry. An innovation patent is targeted at inventions that take an innovative step and have short market lives, lasting up to eight years.

Business schemes and plans are not patentable, nor are abstract business models that happen to involve a new type of corporate structuring to bring about a certain result. However, there are some business methods that are patentable. In order to be patentable, the business method must directly involve a physical device that is used to bring about a useful product. If the method involves the application of technology, the technological aspect must be substantial and a useful product. Related software may only receive patent protection if it meets the requirement for a manner of manufacture, and is an industrially applicable solution to a technological problem.

Fintech businesses may attain copyright protection for the literacy work in source code, executable code and data sets of new software. This usually protects the exact code that causes a computer to bring about a certain result; however, whether this can be extended to the look and feel of the software is debatable.

Broadly, the person or business that has developed intellectual property generally owns that intellectual property, subject to any existing or competing rights. In an employment context, the employer generally owns new intellectual property rights developed in the course of employment, unless the terms of employment contain an effective assignment of such rights to the employee. Contractors, advisers and consultants generally own new intellectual property rights developed in the course of engagement, unless the terms of engagement contain an effective assignment of such rights to the company by whom they are engaged.

Under the Copyright Act 1968 (Cth), creators of copyright works such as literacy works (including software) also retain moral rights in the work (for example, the right to be named as author). Moral rights cannot be assigned but creators can consent to actions that would otherwise amount to an infringement.

i Client data
See Section IV(vi) for further detail on client data and data sharing.
In 2018, the Australian government launched the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (the Royal Commission), which revealed findings of industry-wide misconduct and systemic problems in the operation and processes of Australian organisations and regulators. On 4 February 2019, the Royal Commission made available its Final Report, containing 76 recommendations calling for reforms across banking, superannuation, financial advice and rural lending industries.

Its findings have brought into focus the culture and governance of financial services providers and prompted industry change to prioritise the interests of consumers (and not providers) in the provision of financial services and to address the marked decreased in consumer trust, with 42 per cent of customers acknowledging that trust in banks had deteriorated significantly over the past year. Corporate regulators were also criticised during the Royal Commission for their enforcement practices regarding inaction against corporate misconduct and breaches of the law. Both the Interim Report and Final Report of the Royal Commission commented on the lack of action in response to industry misconduct, noting that conduct was often unpunished or met with penalties that were insufficiently strict. With respect to the two regulators, ASIC rarely took providers to court, and APRA never went to court at all. Given this criticism, it is likely that these regulators will increase their enforcement action in the future and be firmer and more proactive in their responses to misconduct or breaches, rather than reaching negotiated outcomes.

Following the conclusion of the Royal Commission, there has been increased investment in regulatory technology (regtech) and supervisory technology (suptech) by financial services businesses. In 2019, ASIC received government funding for four regtech initiatives to promote Australia as a world leader in developing and adopting regtech solutions to risk management and compliance problems relating to financial services. One initiative included the proof-of-concept chatbox, which is designed to assist businesses in navigating the credit and financial services licensing regulatory framework.

i  **Digital wallets**

The use of digital wallets in Australia has continued to grow. The Council of Financial Regulators (comprising Australia’s major financial regulators) made recommendations to the Australian government for a new framework for stored-value facilities to be overseen by APRA. Stored-value facilities include digital wallets that are increasingly being used as a means of payment and store significant value for a reasonable period of time. The new framework is intended not only to be fit for purpose for the new current financial system but also be able to accommodate future developments and technological advances, such as proposals for global stablecoin ecosystems.

ii  **Asia Region Funds Passport regime**

See Section II(ii) for details of the Passport regime.

iii  **Design and distribution obligations and product intervention powers**

The Treasury Laws Amendment (Design and Distribution Obligations and Product Intervention Powers) Act 2019 (Cth) (the DDOPIP Act) introduces design and distribution obligations in relation to financial products as well as a product intervention power for
ASIC to prevent or respond to significant consumer detriment. The DDOPIP Act, with the exception of Schedule 1, came into effect on 6 April 2019. Schedule 1, which introduces the design and distribution obligations, will commence on 5 April 2021.

iv  Smart contracts

Initially, smart contracts were predominantly used in the cryptocurrency sector in relation to ICOs to automatically mint and distribute tokens. However, in the past 18 months there has been an increase in the institutional adoption of smart contracts to digitise readily automatable processes. This has primarily occurred in the financial services sector with multiparty arrangements such as issuing bank guarantees or debt instruments through smart contracts. The most prominent example of this in Australia is ASX’s proposed replacement of its clearing and settlement system with DLT (see Section VI(v)). Although there is yet to be a widely adopted framework for this, there has been a number of initiatives that aim to develop a framework for the standardisation and regulation of smart contracts such as the Australia’s national science agency, CSIRO’s Data61.

IX  OUTLOOK AND CONCLUSIONS

There has been a variety of regulatory and legislative developments in the fintech industry, and 2020 will likely see changes impacting consumers and businesses. With the outcomes of the Royal Commission and landmark announcements such as ASIC’s decision not to extend licensing relief for FFSPs, the Passport regime and the commencement of Open Banking, fintech is likely to see continued opportunities for growth as the sector moves from speculation to development to implementation.

While the government has a broad commitment to encouraging growth and productivity within the technology and financial services industry, in recent times market regulators have become more focused on consumer education and issued warnings on the risk of trading and investing in new innovations, such as cryptocurrencies. Similarly, following the findings of the Royal Commission, we expect to see more rigorous engagement with ASIC and APRA in the licensing process and a firmer and more proactive approach to enforcement.

Fintechs and start-ups, which historically have emerged to provide consumer focused solutions (powered by technological capabilities) to traditional financial services, can shape new business models to meet increasing demand for bespoke offerings and tailored services, while established institutions continue to face the challenge of redesigning their existing technology platform, strategies and capabilities.
I OVERVIEW

There is currently no special legal regime applicable to fintech companies. Generally, the Austrian financial services market is known for its fairly strict licensing requirements. While not targeted at fintech in particular, depending on a fintech's proposed activities, these may impact its business model. Also, the Austrian Financial Market Authority (FMA) is known for its rather strict administrative practice when evaluating whether market participants provide regulated services without a licence. Fintechs are therefore well advised to carefully scrutinise their business models against regulatory requirements applicable in Austria.

Whereas a ‘regulatory sandbox’ for fintech companies is now part of the current government’s coalition pact (but still needs to be established as law), these businesses are presently subject to the same regulatory and financial services framework as other market participants.

A proposal for a regulatory sandbox has been made by the fintech advisory board of the Austrian Federal Ministry of Finance in 2019. The requirements for being included in the sandbox are (among others) a business model that is based on information and communications technology (ICT), that licensing requirements for business models cannot be excluded and that the business model is (from a technical perspective) already ready for testing. The purpose of the sandbox will be to accelerate the market readiness of such business model in a controlled environment, while the fintech is able to resolve any regulatory issue that may exist at the same time. Applicants will need a business plan evidencing also the fulfilment of all requirements for inclusion in the sandbox. The regulator may grant a temporary banking, MiFID II or PSD II licence for fintech companies included in the sandbox.

Independent of the efforts to establish a regulatory sandbox, the FMA is generally aware of the need for fintechs to obtain legal certainty about the applicable regulatory framework, which can be overwhelming for market participants who are unfamiliar with financial services regulation. The FMA has therefore launched a dedicated web-based platform for fintechs, the FMA FinTech Navigator, which allows fintechs to liaise with the FMA on questions concerning the supervisory laws (e.g., whether a proposed business activity may trigger licensing requirements or the like). Also, in a Q&A-style questionnaire, fintechs can self-check certain standard business models against possible licensing requirements under Austrian law.

---

1 Stefan Paulmayer is a partner at CMS Reich-Rohrwig Hainz Rechtsanwälte GmbH.
The FMA tends to be supportive when approached in a respectful and constructive manner. If a business model is or may be subject to licensing requirements, the FMA will clearly say so. Should this be the case, fintechs should explore potential alternatives, including partnering with licensed market participants (which could act as fronting banks, for example). White-labelling is becoming increasingly relevant for fintechs.

Furthermore, at present there are no special tax incentives available for fintech companies. Fintech start-ups, however, will benefit from the same incentives as other start-ups. These incentives apply inter alia when companies are newly founded and the core of these incentives is relief from certain statutory taxes and stamp duties. Also, there are various institutions providing support (also in terms of funding) to start-ups and fintechs. One such institute is the Austrian Promotional Bank, which has already provided more than €1 billion in funding to start-up companies.

II REGULATION

i Licensing and marketing

Licensing requirements and marketing restrictions will very much depend on a fintech company’s business model and the scope of proposed activities.

Generally, different licensing requirements may apply under the Austrian Trade Code or financial supervisory laws.

The Austrian Trade Code will apply whenever (1) the activity is of a commercial nature and (2) is provided in Austria, as long as no regulated activity is conducted (i.e., because in this case special financial supervisory rules apply). Depending on the activities to be provided, the trade licence may be free or regulated. A regulated trade licence bears additional burdens (such as the requirement to set up a branch or subsidiary in Austria).

If the proposed activities are regulated under financial services laws, specific licensing requirements will apply. In a nutshell, Austria has transposed the relevant EU framework legislation under the Markets in Financial Instruments Directive (MiFID II), the E-Money Directive, the Alternative Investment Fund Manager Directive (AIFMD) and the Payment Services Directive II (PSD II). In addition, as a general guideline, fintech companies should be aware that almost all of the services listed in Annex 1 to the Capital Requirements Directive (CRD IV) require a banking licence in Austria. This may be significantly more burdensome than expected as compared to their home state legislation. For instance, such activities include trading with currencies and financial instruments.

Some typical activities of fintechs have the potential to be licensed or otherwise regulated services: (1) internet platforms or app solutions that offer trading venues for tokens or placement services for tokens, in particular Security Tokens (see Section V.iii); (2) initial coin offering (ICOs), initial token offerings (ITOs) or initial exchange offerings (IEOs); (3) crypto miners in certain circumstances where money is collected from the market; or (4) setting up an investment management company or automated digital advisory company.

Special restrictions on marketing fintech services (besides general requirements under competition laws) generally do not apply as long as the activities are not regulated or the products do not constitute financial instruments or securities. Restrictions will apply if regulated services or securities and financial instruments are involved. It is recommended...
that fintech companies explore specific marketing restrictions that may apply to their specific use case. In particular, marketing via e-mails and cold calling is heavily restricted in Austria. Save for some exemptions (e.g., where the receiver has consented or where previous business relationships exist), generally, no emails may be sent for the purposes of direct marketing.

ii Cross-border issues

The Single European Passport is available for regulated companies under, inter alia, CRD IV, MiFID II, the E-Money Directive, the AIFMD and PSD II. This means that fintech companies that are regulated under their home Member State laws and possess a banking licence, a licence as a payment services provider pursuant to PSD II, a licence as AIFM under the AIFMD, a licence as a-e-money institute or a licence as an investment firm under MiFID II, may passport their licence into Austria and provide their services in Austria without having to first obtain a licence from the FMA.

Where fintech companies do not provide regulated services and are not licensed under their home Member State legislation, no passport is generally available. To the extent that the Austrian Trade Code applies (see Section II.i above), services may be provided in Austria on a temporary basis only under the EU freedom of services without a trade licence. If a service is targeting the Austrian market on a continuous basis or if the services are continuously provided in Austria, a trade licence will be required (see Section II.i above).

Generally, no reverse solicitation exemption will apply (the MiFID II reverse solicitation exemption will only be available to regulated entities from non-EEA Member States). This means that licensing requirements will generally apply when a foreign person is acting in Austria. The FMA’s approach appears to be much stricter than that of the trade authority. As regards regulated services, in order to determine whether a regulated business is conducted in Austria, regulatory practice as applied by the FMA focuses on the place where the offer to enter into a contract is made or where the offer is accepted. As a general rule, market operators will be deemed to carry out licensed banking activities in Austria as soon as any counterparty located in Austria is in a position to enter into relevant, legally binding commitments.

This approach applies irrespective of the means of communication involved. In terms of traditional mail, it will therefore be sufficient if the place of sending and posting the offer to enter into a relevant contract or the acceptance thereof is in Austria. With regard to services offered via the internet, licensing requirements will usually be triggered if clients located in Austria find themselves in the position – technically and legally – to enter into relevant commitments legally binding on them.

This view has further been corroborated by the Austrian Supreme Court in a decision regarding loans granted cross-border by a Swiss bank. Furthermore, case law with respect to a securities portfolio of an Austrian client that was managed outside of Austria (in this instance, the United States) confirmed that advisory services in respect of such portfolio have to be considered to be provided at the place where the customer at the time of provision of these services is located, irrespective of whether such service is provided from outside of Austria via telephone, facsimile, letter, email or similar. Case law further held that the conclusion of an agreement on portfolio management services (to be provided abroad) in Austria was sufficient to conclude that financial services were subject to Austrian licensing requirements.
III DIGITAL IDENTITY AND ONBOARDING

Whereas there is no generally recognised digital identity in Austria, the ‘citizen card’ and a mobile phone signature allow for a secure and authentic electronic signature. A person may officially sign documents via authentication by smartphone app or via a dedicated website. By law, this electronic signature has the same effect as a handwritten signature.

The electronic citizen card and the mobile phone signature is also available to non-Austrian citizens, although the person must be a permanent resident of Austria. The citizen card can be obtained and the mobile phone signature can be activated in various ways, for example, via the online tool of the Austrian tax authorities or in certain Austrian banks or authorities acting as registrars.

Fully digitised onboarding of clients should generally be feasible but will very much depend on the technical infrastructure available. The legal framework for digitised onboarding is set by the FMA in its Ordinance on Online Identification (the FMA Online Identification Ordinance). Many banks use third-party providers to comply with the rather strict standards for online identification set in the FMA Online Identification Ordinance (e.g., conduct of the identification by educated personnel in a separate room with access control, live identification) by way of outsourcing. Such onboarding is most commonly conducted via videoconference, where an operator verifies the identity of the customers in compliance with the FMA Online Identification Ordinance.

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i Payment services

Payment services are regulated under the Payment Services Act, implementing PSD II. Certain services, such as issuing payment instruments or providing money transfers, are regulated and require a payment services licence.

Exemptions as outlined in the PSD II also apply in Austria. The most important exemption relates to the provision of payment services in a limited network. This means, for example, where a payment instrument is only accepted by very few vendors for a specific product (e.g., gas payment cards issued by gas station operators for payment of gas only) or by one vendor for a limited number of products or services or in a limited number of places (e.g., its stores), the issuance of such instruments will not necessarily trigger licensing requirements.

Upon request of the customer, banks are required to provide third parties access to a customer’s account. This was intended inter alia to help fintech start-ups with innovative business models that depend on such data (e.g., platforms for combined access to bank accounts held with different banks).

ii Collective investment schemes

Collective investment schemes are largely regulated under Austrian law in the form of a fund or alternative investment fund (AIF). Depending on how they are structured, collective investment schemes may qualify as undertakings for the collective investment in transferable securities (UCITS) under the Austrian Investment Fund Act or AIFs under the Austrian Alternative Investment Fund Manager Act. An AIF can take whatever legal form possible and is not limited to fund entities similar to UCITS. For instance, some forms of private equity instruments (e.g., shares in private limited partnerships) may qualify as AIFs under Austrian...
law. But also less obvious forms have been deemed as AIF by the FMA: a crypto mining company, for instance, was held to be a AIF. This was based on that mining company offering crypto mining plans to customers where customers could participate in income generated from the company mining certain crypto currencies. When managing or offering an AIF, licensing or registration requirements will apply.

**Securities and investments**

The offering of tradeable securities, such as bearer shares or bonds, is subject to prospectus requirements under the Prospectus Regulation and the Austrian Capital Markets Act 2019 (CMA) supplementing the Prospectus Directive. Exemptions to the prospectus requirements are available.

Furthermore, besides the offering of securities the public offering of investments is also subject to prospectus requirements under the CMA. An investment is the offer of any form of right that is not a tradeable security, provided that a group of persons invests in a project or company or asset and shares the risk associated with the investment. An investment prospectus is considerably less burdensome than a security prospectus and follows the scheme as outlined by an annex to the CMA. Generally, the same exemptions to prospectus requirements as with respect to securities also apply to the offering of investments. Typical forms of investments are, for example, subordinated loans, profit participation rights and limited partnership shares.

If securities and investments are issued below an amount of €5 million, only a simplified prospectus is required and is optional. This simplified prospectus does not follow the schemes under the Prospectus Regulation, but a specific scheme as annexed to the CMA. The advantage of the prospectus being slimmer and less burdensome to produce is, however, accompanied by the disadvantage that passporting of the simplified prospectus into other EEA Member States is not possible. This limits fundraising via such simplified prospectus to Austria, unless the offering of the securities in other EEA Member States is done in reliance on a official exemption from prospectus requirements under the Prospectus Regulation.

**Alternative financing instruments**

Since 2015, the Austrian legislator provides for simplified requirements to funding by way of the Austrian Alternative Financing Act.

The Alternative Financing Act (AFA) was initially introduced to help small and medium-sized enterprises (SMEs) conduct crowdfunding by a set of rules allowing easier access to funding. While donation or rewards-based crowdfunding was not subject to any substantial restrictions, typical crowdfunding campaigns involving the collection of money from the public for investment purposes was usually subject to prospectus requirements under the CMA (see Section IV.ii above).

Subsequently, the AFA was amended and aligned with the CMA. It now no longer distinguishes between the issuance of securities and investments under the CMA on the one hand and the issuance of alternative financial instruments under the AFA on the other. Rather, the AFA now applies to the issuance of securities and investments under reliance on an exemption from prospectus requirements under the CMA. The simplified framework does no longer solely apply to SMEs that are required to use funds directly for their operational expenses. Rather, all sorts of issuers (including licensed entities) are able to make use of the simplified rules.
Under the revised AFA, securities may be issued without the need to prepare a prospectus if the total amount of each issuance does not reach €2 million. This, however, does not mean that such issuances are not regulated. Issuers will need to prepare a key information document that will disclose essential information about the issuer and the relevant project to investors. Still, the burden to prepare a (simplified) prospectus and (with respect to securities) get the prospectus approved by the regulator (FMA) has been lifted – which should help reduce costs for issuers.

Regard must be had to the following restrictions: (1) the aggregate outstanding amount of all investments raised via the AFA may not exceed €5 million over a period of seven years; (2) the aggregate amount of all securities and investments issued pursuant to the AFA may not exceed €2 million over a 12-month period; and (3) the aggregate outstanding amount of all securities and investments in the European Union may not exceed €5 million over a period of 12 months. If by new issuances these thresholds would be exceeded, any such new issuance will require a prospectus under the CMA (see Section IV.ii above). There are limits to the amounts that retail investors may invest in alternative financing instruments (generally €5,000 in a 12-month period), which will need to be taken into account when determining the target market for such an instrument.

Issuers of securities are not bound to rely on the simplified rules. They may continue to prepare a full EU securities prospectus (e.g., when this is beneficial for placement of the securities or the like or passporting of the prospectus is intended); in this case, the rules of the AFA will not apply to such issuances.

iii Lending

Lending is a licensable banking activity under Austrian law. There are no exemptions for peer-to-peer lending or start-up companies; however, the FMA does not appear to pursue private individuals who participate in peer-to-peer lending platforms. It should be noted that the intermediation of loans can also be a licensable banking activity, unless certain exemptions apply, in which case only a regulated trade licence will be required (see Section I above).

Furthermore, factoring is a licensed banking activity under Austrian law. More precisely, the purchase of receivables, including loans, requires a banking licence. The assignment of receivables is also subject to an ad valorem stamp duty in the amount of 0.8 per cent of the assigned value. Certain exemptions to the stamp duty may apply, for example, assignments in the course of a factoring transaction or an assignment of receivables to a securitisation special-purpose entity. No perfection requirements apply with respect to an assignment of receivables. The assignment will be valid once agreed between the parties or in accordance with the terms of the contract. However, a third-party debtor may raise defences and may also declare set-off against the new assignee until being notified of the assignment.

iv Digital marketplaces

Legal requirements for digital marketplaces will depend on the assets that are traded or offered via such marketplaces: where securities are offered and traded, a marketplace could – depending on the exact services offered – qualify as either a stock exchange, multilateral trading facility (MTF) or organised trading facility (OTF). To operate a stock exchange, MTF or OTF requires the operator to be licensed. Unofficially, the FMA has suggested that no such licence would be required since an MTF or OTF requires by definition that the securities are held by a central depository – which is not the case for tokens. In addition, participating in underwriting third-party securities issues as well as related services (third-party securities
underwriting business) is subject to a banking licence under the Austrian Bank Act. Where only investments (see Section IV.ii above) are offered or traded, a regulated trade licence (see Section II.i above) may be required.

In terms of ICOs and cryptocurrencies, a platform will be subject to the above requirements where the coins or tokens are qualified as investment or security (see Section V.iii below). Trading platforms for genuine cryptocurrencies – like Bitcoin and Ether, which do not have an issuer that is collecting money from the public – will usually require no financial services licence but may require a free trading licence (see Section II.i above).

Crowdfunding platforms can be subject to the above licensing requirements – depending on their exact business and services offered. In order to avoid licensing requirements, platforms in Austria have taken different approaches – some do not include securities (including security tokens), while others limit the services so that in fact no licensed service is provided. Often, such platforms are reduced to mere marketing platforms but operators refrain from offering trading (selling or purchasing) securities and tokens or placement of such instruments.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

There is no specific regulation of blockchain technology in Austria. The FMA considers the current legislation to be technology neutral.

i Genuine cryptocurrencies (Bitcoin and Ether)

Cryptocurrencies without an issuer that are generated via a blockchain protocol using mining and distributed ledger technology – such as Bitcoin and Ether – are not considered currencies or financial instruments or tradeable securities in Austria.

This means that trading in such cryptocurrencies is not a regulated activity, but depending on the business model, a trade licence may be required (see Section I above). Nevertheless, if the underlying asset of a derivative instrument consists of cryptocurrencies, this derivative instrument may qualify as a financial instrument under MiFID II. It may be assumed that the same should apply if the value of a token is linked to cryptocurrencies such as Bitcoin or Ether. However, it is not clear that stablecoins linking a token to a fiat currency are treated the same by the FMA. Rather, it appears that the FMA treats such stablecoins as e-money.

Since implementation of the amendment to the EU Anti-Money Laundering Directive (5AML) in early January 2020, the applicable anti-money laundering (AML) rules extend to custodian wallet providers and platforms for exchanging cryptocurrencies. Such providers now need to file a registration with the FMA and must evidence a compliance programme ensuring full adherence to AML rules.

ii Payment token

Slightly different from cryptocurrencies like Bitcoin and Ether, tokens can also take the form of payment tokens that have a similar function to Bitcoin and Ether but are issued by an entity or person.

Currently, some market participants are trying to establish stablecoins that are effectively mirroring a fiat currency such as the euro. Such coins could, for example, be used to pay for goods and services – if the service provider was willing to accept such coins and if some other person was willing to exchange such coins either against fiat currency or potentially also other
types of cryptoassets. Depending on the exact features, such payment tokens could qualify as e-money and issuing such payment tokens may require a licence as an e-money institute. A licence under the Banking Act or the Payment Services Act may be also required, for example, for issuing payment instruments or for providing payment services. There are exemptions from licensing requirements available that would need to be scrutinised on a case-by-case basis.

No securities prospectus (see Section V.iii below) is required to issue payment tokens.

iii Fundraising via tokens

Fundraising via tokens is generally subject to the same rules as any other form of fundraising (see Section IV.ii above). These rules apply when funds are raised in Austria irrespective of whether the issuer or offeror is domiciled in Austria or acting from abroad.

Security tokens

If tokens are structured as tradeable securities, they are most commonly referred to as security tokens and may be qualified as financial instruments and transferable securities, provided such security tokens are freely tradeable in a similar way to securities (presumably the case with any ERC-20 token). Hence, the public offer of such tokens may be subject to prospectus requirements (see Section IV.ii). However, there is also a significant advantage for issuers when tokens are considered as securities, as they will be able to benefit from prospectus passporting rules that would otherwise not be available for initial coin offerings (ICOs) or initial token offerings (ITOs). On the other hand, such qualification might adversely impact certain business models of fintech companies. For example, trading in security tokens may require a banking licence in Austria, advising customers on investments in security tokens might be considered as investment advice under MiFID II, and accepting and transmitting orders for security tokens may also be regulated under the Austrian Securities Supervision Act 2018.

As outlined in Section IV.ii, the offering of investments is also subject to investment prospectus requirements under the CMA. Whenever such investments are represented in token form, particular scrutiny must be applied. This is because the FMA considers investments that are ‘tokenised’ (i.e., issued in token form) to be tradeable securities for the purposes of prospectus requirements (see Section IV.ii). Hence, such tokens also qualify as security tokens. This means that such ICOs/ITOs will require a securities prospectus instead of the more simplified investment prospectus (see Section IV.ii).

All exemptions from prospectus requirement and the easements contained in the AFA should also apply to security tokens and ICOs/ITOs.

Utility tokens

Utility tokens are usually structured like vouchers and grant holders the right to exchange their tokens against goods or services (of the issuer or service partners). Such tokens are qualified as payment instruments by the FMA. However, the FMA considers the limited network exemption under PSD II to be applicable, provided that the tokens are only accepted by the issuer of the tokens and a limited number of service partners (see Section IV.i). Otherwise, a licence under the Payment Services Act, implementing PSD II, may be required.
iv  Tax treatment

*Income tax and capital gains tax*

Cryptocurrencies are treated as immaterial and non-consumable assets for income tax purposes. Interest and gains resulting from cryptocurrencies and tokens are subject to capital gains tax. If held for one's private assets, gains resulting from trading cryptocurrencies are tax-free if the cryptocurrencies are held for longer than one year.

The mining of cryptocurrencies is considered a commercial activity subject to income tax. The same applies to trading cryptocurrencies or operating a Bitcoin ATM.

**VAT**

According to the Austrian Ministry of Finance, in accordance with C-254/14 of the European Court of Justice (Hedqvist), exchanging fiat currency (e.g., the euro) against cryptocurrencies is not subject to VAT. The same applies to cryptocurrency mining.

If goods and services are delivered in exchange for Bitcoin or other cryptocurrencies, the goods and services are taxed the same way as payment effected in fiat currency (e.g., the euro). The amount of tax is calculated in accordance with the value of the cryptocurrency at the time of the exchange.

VI  OTHER NEW BUSINESS MODELS

i  Self-executing contracts

There is currently no special legal framework in place for self-executing contracts (‘if this then that’ (IFTTT)). Any such smart contract would therefore need to fit into existing Austrian civil law rules on contract formation, rights and remedies, enforcement and potential termination or dissolution. When using smart contracts, various legal uncertainties will exist: from the choice of law, to jurisdiction in case of conflict, to questions of warranties and potentially the need to reverse a transaction.

Having in mind the above, smart contracts appear as suitable instruments to execute certain transactions that have been agreed off-chain (e.g., a smart contract to execute a sale and purchase of tokens etc). In such case, the smart contract itself does not establish the obligation but rather the automatism of the smart contract (IFTTT) enables automatic settlement.

Like any other form of contract, if one party wishes to enforce its rights under the contract in Austria, it will need to prove that the other party in fact entered into it. It is largely unclear how such evidence capable of standing up before an Austrian court could be produced in case of self-executing contracts (smart contracts), but this is ultimately a question about what is technically feasible in order to prove the identity of the contracting parties, for example, the implementation of an authentic electronic signature (see Section III).

ii  Fully automated investment process

For licensing purposes under the Austrian Banking Act or the Austrian Securities Supervision Act 2018, it does not matter whether regulated activities are provided in fully automated form or whether an employee is acting on behalf of the investment company. Hence, entities that offer fully automated investment advice or fully automated portfolio management services will also require the respective licences under Austrian law.
iii  Websites comparing products

There is no general rule prohibiting a website that compares different financial products. However, there is a thin line between the mere comparison of the features of regulated products and being seen to offer or market those products to the public. Website operators are well advised to take into account the specific marketing rules in the various legal acts applicable to financial products, including the Securities Supervision Act 2018, the Investment Fund Act or the CMA.

iv  Decentralised exchanges

Decentralised exchanges allow for peer-to-peer transactions between customers without the operator or a central counterparty or intermediary being involved. To the extent that such decentralised exchange facilitates the trading of securities and security tokens, a licence under the Austrian Banking Act or the Securities Supervision Act 2018 may be required (see Section IV.iv).

VII  INTELLECTUAL PROPERTY AND DATA PROTECTION

i  Intellectual property

A business model as such cannot be protected under Austrian law. However, depending on the business model, some aspects relating to it (such as software solutions or inventions necessary to facilitate the business activities) may be subject to protection under local Austrian intellectual property rules:

ii  Patent

Patent protection will be available for all inventions in the technical sector that are new, do not derive from prior art in an obvious manner and can be commercially used.

The Austrian Patent Act excludes certain inventions, products and methods from patent protection, including scientific theories and mathematical methods, aesthetic creative forms, plans and methods for intellectual activities, for games or for business activities and computer programs.

Patent protection grants protection for up to a maximum of 20 years.

iii  Utility patent and design patent

Protection as a utility patent will be available for all inventions in the technical sector that are new, derive from an inventive step and can be commercially used. Excluded from protection are, inter alia, scientific theories and mathematical methods, aesthetic creative forms, plans and methods for intellectual activities, for games or for business activities and computer programs. However, unlike patents, utility patents may also be used to protect programming logic underlying data processing software. A utility patent is granted for a maximum period of 10 years.

Protection as a design patent is available for new and characteristic designs. If a design results solely from a technical function, no protection will be granted. A design patent is granted for a period of five years, which can be extended by further five-year periods up to a maximum term of 25 years.
iv Copyright

Unique intellectual creations are protected by the Austrian Copyright Act. Besides works of art (paintings, films, etc.) and literature, copyright protection may extend to software (including source codes) and databank solutions under Austrian law, provided that these achieve the status of unique intellectual creations. Under Austrian law, the creator is always a natural person. Legal persons cannot be creators within the meaning of the Austrian Copyright Right Act but may, of course, be granted (exclusive or non-exclusive) rights of usage or exploitation.

In terms of software protection, the Austrian Supreme Court held that what is protected is not a work result achieved by a software application, but the individually shaped problem solving achieved by combining many programming steps. A prerequisite for the protection of the programming steps is that they have a certain complexity. In another case, the Supreme Court decided that computer programs have the necessary complexity, for example, if the task at hand allowed for several solutions and the programmer had sufficient freedom of thought to develop individual features. This is to be assumed either in the case of complex programs or if an unusual degree of experience, skill and expertise is manifested in the work. It is also decisive whether a program is newly created or whether the programmer can essentially fall back on already existing program modules.

The copyright ends 70 years after the (last) creator's death.

v Employee inventions

Patents and utility patents

Generally, an employee who creates an invention while being employed by his or her employer nevertheless has the right to patent protection. A contractual arrangement to the contrary is possible but will only be valid to the extent that it concerns ‘service inventions’. A service invention is any invention (1) whose creation was part of the activities that the employee was tasked to provide, (2) which was inspired by the services provided by the employee to his or her employer, and (3) which was facilitated to a substantial extent through use of the resources of the employer.

The employee is nevertheless entitled to appropriate additional compensation for each invention, unless the employee was expressly employed for the purpose of creating inventions for the use of the employer. Ultimately, the employment contract will need to be analysed under labour law to determine whether compensation is owed by the employer to the employee.

The rules applicable to patents will also apply mutatis mutandis to utility patents.

Design patents

If the creation of the design patent was part of the activities that the employee was tasked to provide and the design patent is part of the business area of the employer or if the design patent was created by the employee by order of the employer, the employer will have the right of protection. There is no provision in the Austrian Design Patent Act that would provide for additional remuneration of the employee. Hence, questions of additional remuneration will predominantly be a question of employment or labour law with a specific focus on the contractual arrangement between the parties.
Copyright
An employer will be granted an unlimited right of usage for computer programs that are created by an employee in fulfilling his or her duties in relation to the employer. However, the employee retains the right to be named as the creator. There is no provision in the Austrian Copyright Act that would provide for additional remuneration of the employee. Hence, questions of additional remuneration will predominantly be a question of employment or labour law with a specific focus on the contractual arrangement between the parties.

vi Data protection
Data protection in Austria is governed by Regulation 2016/679 (the General Data Protection Regulation (GDPR)) and by the Austrian Data Protection Act (supplementing the GDPR).

Under the GDPR, personal data that allows for the identification of natural persons is protected and subject to a strict regime. Any person about whom data is processed (the data subject) has certain rights under the GDPR that cannot be derogated from. These rights include the right to obtain transparent information from the controller, the right to obtain rectification of inaccurate personal data, the right to erasure (right to be forgotten), the right to restriction of further processing and the right to object to data processing.

Profiling of client data is part of many fintechs’ business models and is covered by the GDPR. Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is subject to specific regulation under the GDPR, including the right of the client to object.

Under the GDPR, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. This may in particular apply to certain fintechs with business models built on extensive and elaborate data mining, processing or profiling.

Fines under the GDPR are quite hefty and range from between €10 and €20 million and 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is the higher.

In addition, strict banking secrecy applies under Austrian law. All client banking data is protected, even the information that a certain person is a client of a bank. Unlike the GDPR, banking secrecy will also protect legal persons. Any service provider acting for a bank in Austria (e.g., a fintech company providing outsourcing services for a bank) will be bound by banking secrecy by law. Hence, the outsourcing provider will be directly subject to the sanctions of a breach of banking secrecy, including criminal liability.

Data protection and banking secrecy need to be read together – where both are applicable, the stricter standard will prevail. This means that where data processing is permissible under the GDPR but not under banking secrecy, the data processing is not allowed. The same applies vice versa: where data processing is permissible under banking secrecy but not under the GDPR, the data processing is not allowed.
VIII  YEAR IN REVIEW
The past year saw an increased focus on security tokens. As investors shifted away from utility tokens (that do not offer investors any repayment of their capital but rather serve as glorified coupons), start-ups had to consider alternative forms to fundraise via tokens. The predominant capital markets instruments currently being tokenised as security tokens in the Austrian market are profit participation rights. Depending on the exact structuring, such security tokens are often hybrids between debt and equity with the security tokens usually representing a right to a portion of the issuer’s profits.

Currently, the market is seeking ways to offer investors security tokens conferring rights in real properties. Due to the strict requirements of Austrian real property law, usually security tokens are not being able to be directly collateralised by the underlying real property – rather market practice tends to, again, offer profit participation rights in real estate developing companies.

On the regulatory side, a light on the horizon emerged through the draft proposal for a regulatory sandbox (see Sections I and IX).

IX  OUTLOOK AND CONCLUSIONS
Following some turmoil in the Austrian government (which lead to an inactive interim government and new elections in the autumn of 2019), the proposal for the regulatory sandbox outlined in Section I still needs to be enacted into law. As the new government led by the Austrian People’s Party and the Green Party have voiced support for new technologies and in particular blockchain and fintech projects, it is to be hoped that progress may soon be reported.

Meanwhile, depending on a fintech company’s exact business model, licensing requirements may apply. One possible solution for fintech would be to partner with existing and regulated market participants (white-labelling). Any licensable activities would formally be provided by the regulated partner entities, while fintech companies would undertake to provide those entities with specific fintech solutions or act as an outsourcing provider. This would allow them to establish unique and innovative business models while adhering to the regulatory framework. If a business model proves successful, fintech companies could decide at a later stage to seek the required licences themselves.

As all applicable major EU framework legislation (MiFID II, PSD II, 5AMLD) has been implemented, there is currently no further legislation to be expected. However, fintechs and other start-ups can also look forward to the European Commission’s initiative on an aligned European Union crowdfunding regulation. In December 2019, it was announced that the European Parliament’s negotiating team had reached a deal with the Council to allow for cross-border crowdfunding. For amounts up to €5 million, the new regulation shall ease requirements for fundraising, while at the same time ensuring investor protection through a key investment information sheet rather than a full capital market prospectus. While the full text of the final proposal is yet being drafted by the EU’s institutions, the draft proposal very much appears to follow the Austrian sample approach under the AFA (see Section IV.ii above).
I OVERVIEW

i General
Fintech is gaining more and more importance in the Belgian market, especially in light of the presence of EU financial and legislative bodies in Brussels, and because of Brexit. Belgium is also the home of various fintech giants, such as payments system vendor Clear2Pay, smart cash-flow forecasting firm CashForce and the global provider of secure financial messaging services Swift.2 Further, Belgium is the home country of various large market infrastructure players, such as Euroclear, Bank of New York Mellon, Mastercard and Lloyd’s of London.

The majority of the new rules applicable to the fintech sector stem from European initiatives such as:

- Directive 2015/2366 of 25 November 2015 ‘on payment services in the internal market’ (PSD II);
- Directive 2015/849 of 20 May 2015 ‘on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing’ (AMLD IV);
- Directive 2014/65/EU of 15 May 2014 ‘on markets in financial instruments’ (MiFID II); and
- the General Data Protection Regulation (GDPR).

Recently, Belgium has also adopted new legislation targeting alternative funding platforms, which is of particular relevance to crowdfunding platforms.

While the regulatory financial services framework may prove to be quite overwhelming for new and sometimes inexperienced market participants, various initiatives have been taken to guide fintech companies through this jungle of regulations.

ii Legal and regulatory climate
Although many fintech stakeholders have made their case to set up a regulatory sandbox (as in the UK), Belgium has not yet implemented such a sandbox.3 However, the financial regulators have identified fintech as an important focus of their supervisory activities and

1 Pierre E Berger is a partner and Marc Van de Looverbosch is an associate at DLA Piper UK LLP.
3 See, for example, J Latui and E Ponnet, ‘From sounding board to sandbox – the case for a regulatory sandbox in Belgium’ in Bank Fin R 2018, ed. 2, 91.
acknowledge that the financial regulatory framework plays a key role in accommodating both innovation and safety within the industry. Therefore, they have launched a joint FinTech Contact Point, serving as a single point of contact for the financial regulators (as further discussed in Section VI). Companies can raise questions regarding the provision of new and innovative financial products or services requiring a licence. Since its launch in 2016, there have been more than 100 contacts regarding various topics such as robo-advice, crowdfunding, cryptocurrencies, etc.

An important platform fostering and promoting the Belgian fintech sector is FinTech Belgium, a community for financial professionals, start-up entrepreneurs and investors. Apart from promoting the Belgian fintech sector in Belgium and abroad, FinTech Belgium seeks to establish an ongoing dialogue with financial regulators, and regularly organises conferences and seminars on fintech-related topics.

Generally speaking, Belgium can be considered a fintech-friendly jurisdiction.

### iii Tax incentives

#### General

Belgian tax law does not provide for specific tax incentives for fintech companies. Nonetheless, there are several general tax incentives that are beneficial to fintech companies. Some of these measures are described below.

#### Innovation income deduction

Belgian companies are subject to corporate income tax at a rate of 25 per cent as from 2020. The innovation income deduction allows Belgian companies to deduct 85 per cent of the net income that they derive from qualified IP, thus reducing the effective tax rate to 3.75 per cent. Software (original creations or derived works that fulfil a certain originality threshold) that did not generate any income before 1 July 2016 may qualify. In practice, it is advisable to request a binding opinion from the Belgian Federal Science Policy Office (Belspo) about whether the software qualifies. The innovation income deduction is based on a nexus approach, in other words, it will only be available to the extent that the company has itself incurred qualifying R&D expenditures that have given rise to the income derived from the software.

#### Exemption for remittance of professional withholding tax

Companies have the obligation to withhold tax on the salaries they pay to their employees. They must remit the said tax to the Treasury as an advanced payment of the personal income tax owed by the employees. Belgium partially exempts certain companies from that obligation. This measure is aimed at granting these companies more oxygen with regard to cash flow. Micro or small companies that are less than 48 months old are exempt from remitting 10 per cent and 20 per cent of the tax withheld. These companies must fall within the scope of the Belgian Act of 5 December 1968 ‘regarding the collective bargaining agreements’.

A ‘micro’ company does not exceed more than one of the following criteria:

- balance sheet: < €350,000;

---


6 See https://fintechbelgium.be/.
b yearly turnover (excluding VAT): < €700,000; and
c average amount of employees on a yearly basis equal to or less than 10.

A ‘small’ company does not exceed more than one of the following criteria:

- balance sheet: < €4.5 million;
- yearly turnover (excluding VAT): < €9 million; and
- average amount of employees on a yearly basis equal to or less than 50.

Companies involved in R&D activities may benefit from a partial exemption of 80 per cent of the withholding tax on remunerations paid to researchers holding specific academic degrees. This exemption may be limited in the case of certain academic degrees. The R&D programme must be notified to Belspo, and in practice it is advisable to request a binding advice from Belspo relating to the qualification of the R&D programme.

**Tax credit for R&D activities**

Companies investing in R&D may opt to apply a tax credit of 25 per cent. The invested amount is the purchase or investment value of newly purchased or manufactured tangible or intangible assets, which are used for R&D activities in Belgium.

**Tax shelter start-ups and scale-ups**

Individuals who wish to invest in a young company’s equity may recover 25, 30 or 45 per cent of the invested amounts by means of a tax reduction. This measure is aimed at supporting companies’ efforts to raise capital from individual investors. This regime is subject to a series of conditions that must be met by both investors and target companies. The applicable conditions will differ depending on whether the company is between zero and four years old (start-up) or between five and 10 years old (scale-up).

An individual investor cannot invest more than €100,000 per year. Start-ups may not attract more than €250,000 through this regime. Scale-ups are limited to €500,000 (in aggregate with investments gathered previously as a start-up). Investments may be made directly or indirectly through a crowdfunding platform or a public start-up fund.

**Withholding tax exemption for crowd-lending**

Individuals who wish to invest in young, small companies through crowd-lending may benefit from a withholding tax exemption on the first interest income bracket of €15,630. This regime is subject to a series of conditions that must be met by the investors, target companies and the crowdfunding platforms.

II REGULATION

i Licensing and marketing

Financial supervision in Belgium is based on a Twin Peaks model, according to which there are two autonomous supervisors: the National Bank of Belgium (NBB) and the Financial Services and Markets Authority (FSMA). The NBB is responsible for the prudential supervision of individual financial institutions on both macro and micro levels, while the FSMA is responsible for the monitoring of the proper functioning, transparency and integrity
of the financial markets as well as the supervision of unlawful offerings of products and financial services. Furthermore, Belgian banks are fully or partially subject to the supervision of the European Central Bank.

Belgian regulatory law does not provide for a special fintech licence. However, depending on their proposed business model and activities in Belgium, fintech companies may be subject to a licence under general financial regulation. A broad range of activities are regulated in Belgium, mostly stemming from EU legislation. These include, among others, the offering of banking services, investment services, money exchange services, payment services, issuance of electronic money, mortgage and consumer credits, insurance services, reinsurance activities and occupational retirement schemes, as well as the intermediation relating to most of such services. Both the NBB and the FSMA also regularly issue circulars and communications that apply to regulated entities.

Fintech activities in the payment sector are usually within scope of the newly regulated activities of the provision of payment initiation services or account information services under the Belgian legislation implementing PSD II.

Asset management companies are subject to a licence granted by the FSMA under the Belgian legislation implementing MiFID II. In order to be granted a licence, the asset management company has to meet several requirements concerning legal form, capital, adequacy of the shareholder structure, and professional and appropriate management. As of now, there is no specific regulation concerning automated digital advisory in Belgium.

Special regulatory restrictions on marketing fintech services generally do not apply as long as the activities are not regulated or the products do not constitute financial instruments or securities. Restrictions may apply if regulated activities or products are commercialised, for instance under the Information Obligations Decree (as discussed in Section V.ii). Entities are, in general, prohibited from advertising without an appropriate licence. Specific rules also apply where marketing is performed through solicitation in Belgium (see Section II.ii). It is recommended that fintech companies explore specific marketing restrictions that may apply to their specific use case.

ii Cross-border issues

Belgium has implemented the European passporting procedure, which allows firms to conduct activities and services regulated under European legislation in another Member State of the EEA on the basis of an authorisation in its home Member State. Duly licensed entities in Belgium may therefore offer financial services in other Member States after notification to the host Member State, and vice versa. Financial services generally require a licence if they are offered in Belgium (directly or on a cross-border basis). The extent to which the provision and the marketing of financial services trigger licensing requirements under Belgian law should be assessed on a case-by-case basis. According to the Belgian regulators, financial services are being offered ‘in Belgium’ if:

a the financial services are delivered or carried on in Belgium; or
b the financial institution actively solicits orders from customers in Belgium by means of remote sales and marketing techniques or advertising.
III  DIGITAL IDENTITY AND ONBOARDING

i  Digital identity

In Belgium, the government issues an identity card to all citizens that includes a digital identity (eID). The information contained on the eID is deemed official and certified by the government (as certificate authority). An integration with the eID is possible in order to read basic information regarding an individual. This digital identity can therefore be used for onboarding, and can also be used for electronic identification and authentication as well as for embedding a qualified electronic signature on electronic documents.

A number of Belgium’s leading banks (Belfius, BNP Paribas Fortis, KBC/CBC and ING) and mobile network operators (Orange, Proximus and Telenet Group) created a mobile application, itsme, with a view to facilitating such identification, authentication and signatures. Initially, this could only be done on the basis of a Belgian bank account, but it has since been expanded and extended to also support the eID.

The eID is only available to Belgian citizens (irrespective of their nationality) and itsme is only available to holders of a Belgian bank account or a Belgian eID. Because of the eID’s integration of certificates for qualified electronic signatures, it can be used for any contract or document, except specific documents provided for by law (e.g., there are specific conditions for the assignment of certain financial instruments).

ii  Digitised onboarding of clients

In the process of onboarding of clients, ‘obliged entities’ have to assess the risk of money laundering and terrorist financing based on a customer due diligence as set out by the Belgian Act of 18 September 2017 ‘on the prevention of money laundering and terrorist financing and the restriction on the use of cash’ (the AML Act), which implements AMLD IV into national law. Before the establishment of a business relationship or before carrying out of certain transactions, obliged entities are required to identify the customer and verify the customer’s identity, assess and obtain information on the purpose and intended nature of the business relationship and conduct ongoing monitoring of the business relationship.

Digitised onboarding of customers is possible, provided that the relevant entity complies with its KYC requirements under the AML Act. In this respect, the AML Act states that when business relationships or transactions are entered into remotely without any further guarantees (such as electronic signatures), this constitutes an indication of a potentially higher risk. Where higher risks are identified, obliged entities must apply enhanced customer due diligence measures. Further, the entity should set up a process for electronic identification (in particular in accordance with the eIDAS Regulation).\(^7\) The new Anti-Money Laundering Directive\(^8\) (AMLD V) specifically provides that electronic identification means can be used to identify the customer and verify his or her identity if the eIDAS Regulation is complied

---

\(^7\) Regulation 910/2014 of 23 July 2014 ‘on electronic identification and trust services for electronic transactions in the internal market’.

with or if another secure, remote or electronic identification process is used that is regulated, recognised, approved or accepted by the relevant national authorities.\(^9\) The AMLD V should have been implemented in Belgium by 10 January 2020, but thus far has not been.

### IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

#### i Crowdfunding

Various types of crowdfunding platforms exist on the Belgian market:

- **a** platforms through which the public makes a donation for a project or enterprise;
- **b** platforms through which the public deposits money in order to receive a non-financial compensation (reward-based crowdfunding);
- **c** platforms through which the public invests in a project or enterprise through a loan (loan-based crowdfunding, also referred to as crowd-lending); and
- **d** platforms through which the public invests in a project or enterprise through a contribution in capital in consideration for a participation in any profit (equity-based crowdfunding).

Crowd-lending and equity-based crowdfunding are regulated in Belgium by the Belgian Act of 18 December 2016 ‘on the recognition and definition of crowdfunding and containing various provisions on finance’ (the Crowdfunding Act).

The Crowdfunding Act sets out the licensing and operating requirements for alternative funding platforms as well as the conduct of business rules that apply to the providers of alternative funding services. An alternative funding service, dubbed by the FSMA as ‘the financial form of crowdfunding’, is defined in Article 4(1) of the Crowdfunding Act as:

> [T]he service consisting of commercialising investment instruments, through a website or any other electronic means, issued by entrepreneur-issuers, starter funds or funding vehicles in the framework of an offering, public or otherwise, without the provision of an investment service regarding these investment instruments, with the exception of, as applicable, the following services: (i) provision of investment advice and (ii) receiving and transmitting orders.

Each individual or legal entity that professionally provides alternative funding services within the territory of Belgium is deemed an alternative funding platform pursuant to Article 4(2) of the Crowdfunding Act (unless such individual or legal entity is a regulated undertaking).

As regards peer-to-peer lending, the Belgian regulatory framework currently does not explicitly authorise direct lending by consumers to consumers (since individuals are not allowed to make a public call to borrow money).

#### ii Payment services

The offering of payment services is a regulated activity in Belgium under the Belgian Act of 11 March 2018 ‘on the legal status and the supervision of payment institutions and electronic money institutions, the access to the undertaking of payment service provider and

---

\(^9\) See Article 1(8) of the AMLD V.
to the activity of issuing electronic money, and the access to payment systems’ (the Payment Institutions Act), which implements PSD II. The Payment Institutions Act regulates the following payment services:

- **a** services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account;
- **b** services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account;
- **c** execution of payment transactions, including transfers of funds on a payment account with the user’s payment service provider or with another payment service provider (execution of direct debits, payment transactions through a payment instrument and credit transfers, including permanent payment orders);
- **d** execution of payment transactions where the funds are covered by a credit line for a payment service user (execution of direct debits, payment transactions through a payment instrument and credit transfers, including permanent payment orders);
- **e** issuing of payment instruments and acquiring of payment transactions;
- **f** money remittance;
- **g** payment initiation services; and
- **h** account information services.

The exemptions as outlined under PSD II also apply in Belgium. The exemptions that are regularly invoked in the fintech sphere are:

- **a** the limited network exemption;
- **b** the commercial agent exemption; and
- **c** the technical service provider exemption.

Following the implementation of PSD II, banks are required to provide third parties (such as payment initiation or account aggregation providers) access to a customer’s account data, upon the latter’s request. The main reason is to facilitate these new business models that depend heavily on access to such data.

### V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

**i Laws and regulations specifically targeting tokens and cryptocurrencies**

**General**

The FSMA has issued a regulation, a communication, and several press releases and warnings relating to cryptocurrencies or associated phenomena. The NBB has issued a circular. These documents, as discussed in this section, are the only forms of regulatory guidance in Belgium that specifically address tokens and cryptocurrencies.

---

10 On 14 January 2014, the NBB and the FSMA issued a joint press release entitled ‘Be careful with virtual money, such as Bitcoin.’ On 16 April 2015, the NBB and the FSMA issued a joint press release entitled ‘Reminder of the warning by NBB and FSMA against risks attached to virtual money’. On 8 July 2016, the FSMA issued a warning relating to OneCoin, a cryptocurrency. On 13 November 2017, the FSMA issued a press release entitled ‘Be wary of Initial Coin Offerings (ICOs)’, which accompanied the FSMA ICO Communication discussed above. On 22 February 2018, the FSMA issued a warning entitled ‘Cryptocurrency trading platforms: beware of fraud!’ The FSMA has also put together a regularly updated
In a motion for a resolution dated 18 July 2019 and tabled again on 8 October 2019, seven Belgian senators urged the Belgian government to adopt a legal framework for the sale, purchase and use of virtual money and related financial products, in order to protect consumers and to fight the use of these virtual currencies for criminal purposes. The motion was discussed in a hearing before the Committee on Cross-cutting Issues on 31 January 2020, where the Chairman of the FSMA, Jean-Paul Servais, provided information on cryptocurrencies.11

**Marketing Prohibition Regulation**

On 3 April 2014, the FSMA issued the Regulation of the Financial Services and Markets Authority of 3 April 2014 ‘on the prohibition on marketing of certain financial products to non-professional clients’ (the Marketing Prohibition Regulation), which entered into force on 1 July 2014.12 This regulation prohibits the professional marketing in Belgium to one or more retail clients of financial products, the return of which is directly or indirectly dependent on virtual money. ‘Virtual money’ is defined for the purposes of the regulation as ‘each form of non-regulated digital money without legal tender’. This definition comprises not only Bitcoin, but also other cryptocurrencies. The prohibition only applies in respect of derivatives of virtual money, not in respect of the virtual money itself.13

**Circular NBB_2019_20**

On 13 March 2019, the Basel Committee issued a ‘statement on cryptoassets’. In this statement, the Basel Committee warns of the risks related to cryptoassets. It then sets out the measures it expects banks to take if they acquire cryptoasset exposures or provide related services.

As a follow-up to the Basel Committee’s statement, the National Bank of Belgium (NBB) released Circular NBB_2019_20 ‘on expectations regarding activities related to cryptoassets’ on 19 July 2019.14 This is addressed to the financial undertakings under the NBB’s supervision. The NBB deemed that the substance of the Basel Committee statement was also relevant for other financial undertakings. It therefore decided to issue Circular NBB_2019_20 to reiterate the Basel Committee’s statement and to extend its scope to also include non-banks under its supervision.

**FSMA ICO Communication**

On 13 November 2017, the FSMA issued a communication entitled ‘Initial Coin Offerings (ICOs)’ (with document number FSMA_2017_20: the FSMA ICO Communication).15 In this text, which is considered soft law, the FSMA endorses the statements by the European

---

12 Approved by the Royal Decree of 25 April 2014 ‘approving the regulation of the Financial Services and Markets Authority regarding the prohibition on marketing of certain financial products to non-professional clients’.
13 Robby Houben, ‘Bitcoin: there are two sides to every coin’ (2015) 2 TBR 139, 154 Paragraph 34.
Securities and Markets Authority (ESMA) on ICOs, in which ESMA has determined that, depending on how ICOs are structured, various financial regulations, such as the Prospectus Directive, MiFID, AIFMD, MAR, AMLD IV, etc., may apply.\textsuperscript{16} The FSMA further states that the following legislation and regulations may apply to ICOs in Belgium:

\begin{itemize}
  \item[a] the Act of 16 June 2006 ‘on public offers of investment instruments and the admission of investment instruments to trading on regulated markets’ (the Old Prospectus Act). Meanwhile, however, the new Prospectus Regulation (2017/1129) has been implemented in Belgium by the Act of 11 July 2018 ‘on the public offering of investment instruments and the admission of investment instruments to trading on a regulated market’ (the New Prospectus Act). The New Prospectus Act will fully apply, and will fully repeal the Old Prospectus Act, as from 21 July 2019;
  \item[b] the Marketing Prohibition Regulation (discussed above); and
  \item[c] the Crowdfunding Act (discussed above).
\end{itemize}

The FSMA notes in its communication that the application of the above laws depends on the way in which the ICO in question is structured, and that this must be assessed on a case-by-case basis. While the FSMA does not expressly mention the criteria it may apply when undertaking this assessment, it does point out elsewhere in the communication that:

\begin{quote}
[i]he characteristics of a token may be similar to: (i) investment instruments, given that they may provide rights, offer the prospects of revenues or returns, or involve a pooling of funds with a view to investment in tokens; (ii) a means of storage, calculation and exchange, given its convertibility into other tokens, cryptocurrencies or fiat money; and/or (iii) a utility token, given the access which the token provides to the product or service.
\end{quote}

This corresponds to the classification of tokens and cryptocurrencies as either: (1) an investment token; (2) a cryptocurrency; or (3) a utility token; or any combination of these three variations, which is gaining traction among scholars and policymakers.\textsuperscript{17} Whereas thus far this trichotomy constitutes a merely descriptive classification, it can already provide a sense of the likelihood that the coin will fall within the ambit of one or another law (such as one of the laws discussed in the next section).

\section{General laws and regulations that may apply to tokens and cryptocurrencies}

\subsection*{General}

Save for the Marketing Prohibition Regulation, there are no Belgian (hard) laws or regulations that specifically target blockchain or cryptocurrencies. Consequently, any type of cryptocurrency, token or other asset created or transferred by means of distributed ledger technology, as well as any related service, must be analysed from the perspective of existing laws and concepts. Most Belgian financial laws, including anti-money laundering laws, do not materially deviate from the EU legislation they seek to implement, and will therefore not be discussed here. There are, however, some interesting deviations from or additions to the EU financial law framework, a selection of which are discussed below.


**Prospectus regime**

The Belgian prospectus legislation, among others:

*a* deals with the requirement of preparing a prospectus to be approved by the FSMA or an information note in the event of a public offering of investment instruments within the territory of Belgium;

*b* establishes a monopoly on intermediation for the placement of investment instruments within the territory of Belgium; and

*c* determines that advertisements used in connection with the public offering must receive prior approval from the FSMA.

Unlike the old Prospectus Directive (2003/71/EC) and the new Prospectus Regulation (2017/1129), both the Old Prospectus Act and the New Prospectus Act do not use the notion of ‘securities’ to determine the material scope of the prospectus regime. Instead, they use the significantly broader notion of ‘investment instruments’. This latter concept includes securities, but also comprises a whole range of additional instruments (such as money market instruments, futures, forward rate agreements and equity swaps), as well as the residual category of ‘all other instruments that enable a financial investment, irrespective of the underlying assets’.

Consequently, depending on the structure of the token issued in an ICO, there may be a high chance that the token qualifies as an investment instrument and therefore falls within the scope of the Belgian prospectus regime.\(^\text{18}\)

The Belgian prospectus legislation also establishes an intermediation monopoly. Only the entities mentioned in Article 21, Section 1 of the New Prospectus Act, which are all regulated entities, are allowed to act as intermediaries for purposes of the placement of investment instruments within the territory of Belgium. Consequently, if a token qualifies as an investment instrument and is placed in Belgium, only regulated entities can act as intermediaries (with certain limited exceptions).\(^\text{19}\)

**Consumer protection**

If a token qualifies as an investment instrument for purposes of the prospectus legislation discussed above, the token will also qualify as a financial product and will thus fall within the ambit of, in particular, the Royal Decree of 25 April 2014 ‘on certain information obligations in respect of the marketing of financial products to non-professional clients’ (the Information Obligations Decree).\(^\text{20}\) As its name suggests, this Decree provides for certain information obligations that must be complied with when professionally marketing financial products to retail clients.

Furthermore, when the service offered in respect of a token or cryptocurrency qualifies as a financial service, Book VI of the Belgian Code of Economic Law, containing various

---

\(^{18}\) Robby Houben, ‘Bitcoin: there are two sides to every coin’ (2015) 2 TBR 139, 150 Paragraph 23; Niels Vandezande, Virtual Currencies: A Legal Framework (Intersentia 2018) 333. For an analysis under EU law, including the exemptions that may apply (also under Belgian law), see Philipp Hacker and Chris Thomale, ‘Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law’ (2018) 15 ECFR 645, 657–689.

\(^{19}\) Robby Houben, ‘Bitcoin: there are two sides to every coin’ (2015) 2 TBR 139, 152 Paragraph 30; see Articles 20–21 New Prospectus Act.

consumer protection provisions, applies. A financial service is defined in this Code as ‘each banking service or service relating to lending, insurance, individual pensions, investments and payments’.

iii Tax treatment

Corporate income tax
The Office for Advance Tax Rulings has recently confirmed that all gains from investments in cryptocurrencies and ICOs made by Belgian companies are taxable, and all losses are tax deductible.

Personal income tax
The income tax treatment of investments in cryptocurrencies by individuals is subject to general tax rules and depends on the relevant facts and circumstances.

A capital gain realised within the framework of one’s professional activity will be taxed as professional income at progressive rates ranging between 25 per cent and 50 per cent plus local charges. If the cryptocurrencies are held as private assets, the capital gains will be exempt from individual income tax if the sale qualifies as a normal act of management. If not, the capital gains will be taxable as miscellaneous income at a rate of 33 per cent plus local charges.

Legal certainty on the applicable tax treatment can be obtained by filing a ruling request with the Office for Advance Tax Rulings. The said service has recently published a list of questions that should allow both the taxpayer and the tax authorities to determining the appropriate tax treatment.22

VAT
As regards VAT, the European Court of Justice (Skatteverket v. David Hedqvist, C-264/14, dated 22 October 2015) has ruled that the sale of non-traditional currencies falls under the same exemption as for transactions relating to traditional currencies. The Belgian VAT administration has included that decision in its administrative commentary without noteworthy remark.

VI OTHER NEW BUSINESS MODELS

i Smart contracts
Self-executing contracts, or ‘smart contracts’, are in principle permitted under Belgian law. No specific legal framework has been established for this phenomenon. Therefore, common contract law applies. In Belgium, contracts can generally be concluded without formal requirements, subject to certain statutory exceptions (e.g., consumer credit contracts). The computer code making up a smart contract can thus in principle constitute a valid contract,

21 Robby Houben, ‘Bitcoin: there are two sides to every coin’ (2015) 2 TBR 139, 153 Paragraph 32.
22 See https://www.ruling.be/fr/telechargements/liste-de-questions-crypto-monnaies.
provided the validity requirements under Belgian contract law are met. Some tentative attempts to analyse smart contracts under Belgian contract law have thus far been made, but a considerable degree of legal uncertainty remains.

ii Robo-advice

Automated investment advice, or ‘robo-advice’, is relatively popular in Belgium. Within Europe, Belgium has the third-largest national portfolio, with €386 million invested with robo-advisers, equivalent to €34 per capita. According to Roland Berger, the Belgian market is expected to grow significantly to €3.7 billion assets under management by 2022. Financial regulation, such as MiFID II, apply to automated investment advice as they do for non-automated investment advice. This sometimes causes slight vexation among market participants, who feel that regulatory requirements are applied too strictly to online platforms.

Third-party websites comparing products or providing information about financial products are subject to data protection and competition rules. The vast majority of these rules are of EU origin. The GDPR applies and must be taken into account when users’ personal data are being processed. Also, comparison platforms are in particular subject to the regime of Article 101 TFEU and the EU regulations and case law in this respect.

iii Fintech contact point

For new business models in the fintech realm, the FSMA launched a FinTech Contact Point in June 2016. This contact point is designed as a portal through which fintech entrepreneurs can contact the financial supervisor. This allows entrepreneurs to familiarise themselves with financial legislation and to ask any questions they may have. It also enables the FSMA to closely monitor fintech developments in Belgium. In April 2017, the portal launched by the FSMA evolved into a joint portal of the FSMA and the NBB. Fintech players, who are not necessarily aware of the Twin Peaks supervision model in Belgium, thus have a single point of contact; they do not need to find out in advance to which supervisor they need to ask their questions. Questions lodged with the fintech portal are managed jointly by the FSMA and

---


26 id.

27 See, for instance, the MeDirect Bank responses to the questions (in particular question 5) asked to market participants in the context of the Discussion Paper on automation in financial advice of the Joint Committee of the three European Supervisory Authorities (EBA, EIOPA and ESMA), 4 December 2015, available at https://eba.europa.eu/news-press/calendar?p_p_id=8&_8_struts_action= per cent2Fcalendar per cent2Fview_event&8_eventId=1299860.

Belgium

NBB teams. Since the launch of the fintech portal in 2016, over 100 fintech entrepreneurs have reached out to the supervisory authorities. Their questions covered a wide range of topics, such as cryptocurrencies, robo-advice, crowdfunding and price comparison.29

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

i Intellectual property

Anything that is not a technical solution, including schemes, rules and methods for performing mental acts, playing games or doing business, and software as such, is excluded from patent protection. This does, however, not preclude software-based inventions that are implemented in hardware from patent protection, provided that all applicable conditions are fulfilled.

Software and business models may also be protected by copyright if they meet the originality requirement. For acquiring copyright protection, no formalities need to be fulfilled. Only the expression of the software or business model will be protected, and not the underlying ideas or principles.

The object and source code, architecture, structure and organisation of the software are considered the ‘expression of the software’. A graphic user interface does not enable the reproduction of the software, and is therefore not considered an expression of the software. Consequently, a graphic user interface cannot be protected under the Software Act, but only by common copyright law.

Unless otherwise specified in the employment contract, the employee that is the creator of an original work will own the copyright on that work. The same applies to contractors. With regard to software, however, there is a legal presumption that the employer is the copyright owner of the original software created by the employee.

No specific compensation regime is provided for by law, allowing parties to freely agree on a potential compensation for any intellectual property created.

ii Data protection

Fintech companies that are based in the EU, or that offer goods or services to natural persons (data subjects) in the EU or monitor their behaviour, will have to comply with the principles and obligations of the GDPR and the Belgian Act of 30 July 2018 when processing personal data. If the client data consists of information relating to an identified or identifiable data subject, the data will be qualified as personal data.

Profiling refers to the creation and use of profiles of data subjects based on common characteristics (e.g., preferences, financial status). Depending on the objective of the profiling, it will be treated differently. The use of profiles to create recommendations and personalise the client experience, for instance, will not be treated the same way as the use of such profiles to automatically reject credit applications or otherwise significantly impact the rights of the data subject.

In the first scenario, in other words, a mere scoring or evaluation, the general rules of the GDPR will apply, and the specific requirements to carry out a data protection impact assessment (DPIA) may apply in Belgium (as well as elsewhere), depending on the other


© 2020 Law Business Research Ltd
circumstances of the processing (e.g., data enrichment via other sources, scale of processing). For the second scenario, a DPIA will in any event be required under the GDPR, and specific requirements apply in relation to the permitted legal grounds for such processing, the categories of personal data that may be taken into account and data subject rights.

In each scenario, a risk assessment will be needed to determine whether the supervisory authority must be consulted in relation to the project.

**VIII YEAR IN REVIEW**

The most relevant developments in the regulation and legal treatment over the past 18 months came as a result of European directives and regulations. The implementation into Belgian law of recent EU legislation, such as the AMLD IV, PSD II and MiFID II, has had an important impact on fintech companies. Furthermore, the entry into force of the GDPR has required fintech companies to put GDPR compliance programmes in place to safeguard the rights of individuals.

At the national level, the recent Crowdfunding Act provides a regulatory framework for alternative financing services. Both crowdfunding and crowd-lending platforms need a licence from the FSMA under this Act. As a result of the Crowdfunding Act and multiple tax incentives, the Belgian crowdfunding market has shown significant growth in 2017.30 It is expected that this market will continue to develop and grow in the future.

**IX OUTLOOK AND CONCLUSIONS**

Although there is no regulatory sandbox in place, and there are, to our knowledge, no plans to introduce such a sandbox, Belgium can be seen as a fintech-friendly jurisdiction.

The Fintech Contact Point will continue to be helpful in guiding start-ups and established firms through the complex regulatory framework and the licensing process. Both the FSMA and the NBB tend to be approachable and supportive of new fintech business models, and we expect this to only increase in the future.

The AMLD V, which should have (but has not) been implemented in Belgium by 10 January 2020, will also have an impact on fintech companies, as it will acknowledge the use of electronic identification means, and address the risks linked to virtual currencies.

---

Chapter 4

BRAZIL

Alexei Bonamin, Marcela Waksman Ejnisman, Carla do Couto Hellu Battilana, Marcus Fonseca, Felipe Borges Lacerda Loiola, Natasha Wiedmann and Victor Cabral Fonseca

I OVERVIEW

Brazilian financial technology (fintech) has developed considerably in recent years. The latest version of FintechLab Radar (June 2019) demonstrated a growth of 30.9 per cent in the number of total companies acting in this market, compared with the previous edition published in August 2018. According to the mapping created by the publication, Brazilian fintech operates in 11 different sectors: payments, financial management, credit and loans, investment, insurance, funding, digital banks, debts, cryptocurrencies, exchange and multiservices. Among these, the payments and loans sectors performed the highest growth rates – 43 per cent and 36 per cent respectively.

This diversity of the ecosystem shows the strength of the financial technology market in the country. Given this scenario, Brazilian regulatory entities demonstrated a strong interest in knowing such players and, in some cases, already published specific norms for some of their activities. National laws and governmental entities, such as the Central Bank of Brazil (BACEN) and the Brazilian Securities and Exchange Commission (CVM), regulate the Brazilian financial system. Other agencies also have regulatory power in specific areas, such as the Private Insurance Superintendence (SUSEP) for the insurance industry.

Some initiatives that have already resulted in or are about to become Rules that can directly affect fintech exemplifies the agencies’ regulatory interest. This is the case, for example, of CVM Rule No. 588/2017, which provides standards for the investment-based crowdfunding industry in the country or the proposals for peer-to-peer lending and crowd-lending regulations, currently before the BACEN (Public Hearing No. 55/2017). In addition, the same government agencies conduct studies on the fintech sector, as evidenced by the creation of the CVM’s Fintech Hub of Innovation in Financial Technologies.

The development of specific innovations in the financial sector is notable, more specifically in the areas of credit and payment, which are showing consistent showing a significant growth. The year 2018 was marked by the regularisation of peer-to-peer lending (P2P) in Brazil, through Central Bank Resolution No. 4,656/2018, which regulates financial institutions that use electronic platforms to connect creditors and debtors (SEPs) or to lend their own resources (SCDs). In addition, in 2019 the BACEN structured an instant payment architecture that will replace the current resource transfer system in November 2020. With the start of the new protocol, such transfers will be made instantly and will be available 24 hours a day, all year round.

1 Alexei Bonamin, Marcela Waksman Ejnisman and Carla do Couto Hellu Battilana are partners, and Marcus Fonseca, Felipe Borges Lacerda Loiola, Natasha Wiedmann and Victor Cabral Fonseca are associates at TozziniFreire Advogados.
Although there is no regulation of the whole fintech sector, nor any tax incentives, there has been a significant increase in the activities, which are becoming increasingly relevant to the market. In this sense, regulatory agencies are promoting a fintech-friendly policy, this being their major objective to ensure the integrity and security of financial operations.

There are broader legislative discussions about what is known as the ‘Start-up Point’, a package of laws and regulations that could bring a series of benefits not only to fintechs, but to all companies that fit the definition of ‘start-up’. Such benefits will be of a labour, tax, corporate and investment nature, among others. However, there is still no certainty about when or how these new rules will be implemented; in 2019, the Brazilian government held several meetings with the private sector in order to raise demands and map possible incentives. Further developments are expected to occur in 2020.

In addition, Law No. 13,709/2018 – the Brazilian General Data Protection Law (LGPD), inspired by international guidelines and legislation, especially the EU General Data Protection Regulation, was enacted in August 2018 and will become effective from August 2020. The LGPD applies to any processing of personal data, by public and private entities, in the online and offline environments, using automated and non-automated means – reaching, therefore, the activities of fintech companies involving the handling of personal data.

Thus, it is possible to consolidate the regulatory and policy approach for fintech companies considering that while the financial sector itself is heavily regulated, state entities have been adopting a benign and favourable view of the development of tech-based financial enterprises so far. Their actions demonstrate that developing an innovation-driven economy may be one of the main goals for the next years.

II REGULATION

i Licensing and marketing

Brazilian legislation does not provide a specific type of operating licence for fintechs. In practice, the nature of the services offered by these companies will dictate which rules are applicable to them, such as those of a particular economic sector.

Most of these rules are enacted by entities that are part of the National Financial System (SFN), whose competences are fixed in Article 192 of the Federal Constitution of 1988. The SFN is divided into three main organs and their respective operating sectors:

a the National Monetary Council, which regulates currency, credit, capital and exchange;
b the National Council for Private Insurance, responsible for private insurance; and
c the National Council for Complementary Pension, which regulates closed pension funds.

Within each sector there also supervisory bodies:

a the BACEN, which regulates financial institutions, money, credit, payments and exchanges;
b the CVM, responsible for the regulation of securities, commodities and futures;
c SUSEP for the insurance industry; and

---
2 For a detailed description of the composition of the National Financial System and functions of each entity, see www.bcb.gov.br/Pom/Sph/Ing/InstitucionalAspects/TheRoleFinancialIntermediaries.asp (in English).
Thus, a fintech operating in Brazil needs to observe, in addition to the general laws, specific rules that affect the markets in which it operates, established by the competent bodies.

In this way, even if there is no special licence for fintech companies to function in the country, the services or products they offer – or even the market in which they operate – may determine whether their businesses require any particular authorisation or if there are specific rules for such activities. Financial institutions such as banks, for example, may only operate in the country if authorised by the BACEN and if they comply with certain requirements, such as the obligation to be constituted as a sociedade por ações (a commercial partnership whose capital stock is divided into shares and in which each shareholder has a limited responsibility according to the sum of money he has invested) or other rules envisaged by the financial authority.

Another heavily regulated sector of fintech is the securities market. In this sector, the CVM provides rules for many services related to the trading of securities and related activities. The agency controls and regulates, among others, capital markets and investment funds (CVM Rules No. 400/2003, 476/2009, 555/2014 and 578/2016, and others), asset management (the most important being CVM Rule No. 558/2015) and investment advisory services (represented by the recently edited CVM Rule No. 592/2017). The use of automated systems or algorithms is permitted for both asset management and advisory activities.

Another industry commonly associated with fintech is investment-based crowdfunding, which is regulated according to CVM Rule No. 588/2017. Following international standards, the norm established the rules for the operation of collective financing platforms and determines that if some precedent requirements (set forth in the law) are present, the distribution of certain securities is exempt from registration before the entity, which is usually very costly for the issuing company.

Thus, some securities-related sectors in which fintech is present – such as robot advisers and investment-based crowdfunding platforms – are regulated by the CVM and companies that operate in these sectors must observe the rules issued by the CVM.

The Consumer Protection and Defence Code equates banking, financial, credit and insurance services to the general delivery of services. Consequently, consumer protection law applies to service suppliers such as banks or credit institutions, if it is possible to verify a consumer relationship between them and the clients.

One of the outcomes of this legal treatment is the existence of rules regarding credit information services. The Code states that consumer databases must be objective, clear, created in a language that is easy to understand and may not contain negative credit information relating to a period exceeding five years. Upon a consumer’s request, inaccurate and outdated

---

3 Law No. 4.595/64, which creates the Brazilian National Financial System, determines some specific rules for the operation of financial institutions and other players within this market.
4 Such as BACEN Resolution No. 4.122/2012, that establishes the procedures for the licensing and authorisation granting multiple kinds of banks.
5 Article 16-A, CVM Rule No. 558/2015.
6 Article 16, CVM Rule No. 592/2017.
personal information must be corrected within five business days. Consumers are further entitled to access their personal information and request their exclusion from a database, except for credit information relating to a period of less than five years.

ii Cross-border issues

In general, Brazilian law does not prohibit the offering of financial products or services, only regulating the way certain transactions need to be conducted. As described, the SFN is composed of several entities, each with specific competence in relation to activities of a financial nature. In this way, it is necessary to understand the nature of the service or product offered by the fintech company to verify if there is any requirement for foreigners to operate in the country.

Any activity developed in Brazil is primarily subject to national legislation. However, some international entities rulings may guide the standards of the national regulations, since Brazilian authorities are part of many transnational organisations such as the Basel Committee on Banking Supervision and IOSCO, for example. Recent legal initiatives also considered international experience, as the Investment-based Crowdfunding Rule (CVM Rule No. 588/2017), which is inspired by the regulatory approach used in Israel, France, the United Kingdom, the United States, Portugal and Canada, among others. Another relevant recent regulatory change is CVM Rule No. 619/2020, which allows for securities-related investment advisers to have their domicile abroad and is a result of the understandings established between Brazil and the Organisation for Economic Co-operation and Development (OECD) aiming to align Brazil with the OECD’s Codes of Liberalisation of Capital Movements and the Brazilian market with international best practices.

Some activities are restricted to financial institutions (banks), such as the custody of third-party resources and the intermediation and application of their own or third-party financial resources. In these cases, it is necessary to comply with the banking regulation in the country, which determines that foreign banks may operate in Brazil if registered within the BACEN and explicitly authorised by a decree enacted by the President of the Republic.

In other situations, if the fintech provides any securities-related products or services, its activities are subject to the CVM Rules. The management of securities portfolios (asset management), for example, can only be done by a natural person or legal entity headquartered in Brazil and authorised by the CVM.

Finally, the inflow and outflow of funds to and from Brazil is permitted, since individuals and companies are free to send money abroad and realise investments of any nature offshore. However, these transactions must be completed through Brazilian financial institutions authorised by the BACEN to operate in the foreign exchange market. Those institutions are under the supervision of the Brazilian financial authorities and thus must comply with know-your-customer (KYC) and anti-money laundering provisions contained in Brazilian regulation, including identification of the ultimate beneficial owner of the corporate structure. Moreover, the BACEN issues an annual basis regulation determining that any Brazilian holding investments abroad of an amount higher than a given threshold shall declare this investment to the BACEN for statistical purposes. In addition, capital gains obtained abroad will be subject to taxation as provided for in Brazilian tax law.

---

7 Amending CVM Rule No. 592/2017.
8 See Law No. 4,595/1964.
9 Among other prerequisites. See CVM Rule No. 558/2015.
III DIGITAL IDENTITY AND ONBOARDING

In Brazil, there are various types of identification documents, but many of them can be substituted with a driver's licence that can be transferred onto a digital version. The paper document will not be discontinued and is still mandatory as a driving permission, but now citizens can conveniently carry a digital copy on their smartphones.

It is worth mentioning that Federal Law No 13.444/2017 created the national identity document (DNI), a digital document that will waive the obligation imposed on citizens to hold, as the case may be, documents such as birth and marriage certificates, voter registration and taxpayer registry identification. Nonetheless, the DNI is still under development and has not been implemented yet. Meanwhile, Presidential Decree No 9.723/2019, issued in February 2019, mandates that the taxpayer registry identification number is sufficient for identification purposes for access to information, services and the exercise of rights or benefits. Although this rule is destined exclusively for identification before executive entities, it may reflect on the practices of other institutions, private or public, that might want to simplify identification procedures.

As of the use of documents by financial service providers, BACEN Resolution No. 4.474/2016 authorises institutions to discontinue the use of physical copies once they are digitised and secured within their systems. The only change with regard to digital onboarding comes from BACEN Resolution No. 4.753/2019, in force since 1 January 2020, which establishes rules for opening and closing of deposit accounts (such as current, savings or salary accounts), simplifying the procedure and allowing for clients to request the aforementioned services through any service channels provided by the financial institution except through a phone call.

According to the new Resolution, financial institutions must adopt procedures that allow for the verification of the account holder's identity and of its representatives, as the case may be, as well as the authenticity of the information provided by the clients.

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i Crowdfunding

The law regulates transactions involving securities and, therefore, this market has specific rules established by the agency responsible for overseeing it: the CVM. Brazilian law adopts an open concept for security, considering as such any title or collective investment scheme that generates the right to participation, partnership or remuneration, which income is originated in the effort of entrepreneurs or third parties, including the ones resulting from the rendering of services. If any specific collective investment scheme falls under this description, it is subject to the determinations of the law and the CVM Rules, which may regulate how they are distributed, offered and commercialised inside Brazilian territories or abroad, if the investment schemes are issued by Brazilian companies. All regulations regarding the SFN apply to fintech organisations, if legally prescribed services or products are offered.

Nonetheless, Brazilian authorities have legally recognised investment-based crowdfunding as a possible fundraising option for small companies. Currently, the Brazilian

---

10 As described in Article 2, IX, Law No. 6.385/1976.
11 Companies which have an income of 10 million Brazilian reais or less, as defined by Article 2, III, of CVM Rule No. 588/2017.
innovation ecosystem benefits from CVM Rule No. 588/2017, enacted specifically to regulate the distribution of securities through platforms established for this purpose, without the need to register the offer before the CVM – which, as explained above, is the general rule and might be very expensive for small companies. The Rule came into force in 2017 following a market public consultation conducted by the CVM, and its current version establishes some requirements and responsibilities for the operation of the platforms, details the possible offers and recognises the possibility of syndicated investments, that is, those led by an investor well known in the market.

ii Intermediation of loans and lending models – P2P lending and crowd-lending

The intermediation of loans is a private activity of financial institutions, as determined by the law that constitutes the SFN. Thus, any organisation that collects money from third parties for loans or intermediate transactions of this nature must be registered and authorised to operate as a financial institution according to Brazilian law and is subject to the supervision and regulation of the BACEN. In order to foster innovative lending models, in 2017, the BACEN proposed a public hearing to deal with P2P lending and crowd-lending, seeking to guarantee the safety and legality of such loans. As a result, in April 2018, the BACEN published Resolution No. 4656/2018, which created two special types of financial institutions, allowing them to use SEPs or SCDs. Both need to request an authorisation to operate before the BACEN. Nonetheless, the authorisation procedure used by these institutions is easier and faster than the one required by traditional financial institutions.

iii Payment services

Payment services are subject to the rules regarding the Brazilian payment system (SPB), created by Law No. 10,214/2001, and to the supervision of the BACEN. The SPB comprises services or systems that, subject to authorisation by the competent authorities, may:

- clear credit notes;
- clear and settle electronic debit and credit orders;
- transfer funds and other financial assets;
- clear and settle securities transactions; and
- clear and settle commodities and future transactions.

In 2018, the BACEN enacted regulations with the expectation to promote financial inclusion, as well as enabling a more competitive market through the SPB. BACEN Resolution No. 4707/2018 and Circular No. 3924/2018 regulate the use of payment arrangement receivables as collateral for credit transactions. This should make lending to smaller companies feasible, as such receivables usually represent a significant portion of their assets, and the creditor will be granted more protection when entering into contracts with them.

The aforementioned rules will be valid only until 3 August 2020, when Resolution No. 4734/2019 and Circular No. 3952/2019 will become effective, replacing the current regulation applicable to the aforementioned kind of collateralised transactions. The new rules incorporate principles and dispositions contained in BACEN Resolution No. 4707/2018 and

---

12 CVM Rule No. 588/2017.
13 These organisations’ descriptions may be translated to ‘peer-to-peer lending company’ and ‘direct loans company’, respectively.
Circular No. 3,924/2018 while also introducing several modifications related to registration of receivables of credit and debit payment instruments. As soon as they enter into force, financial institutions will have to ensure that receivables from payment arrangements used as collateral for their credit transactions or assigned in discount transactions are recorded in registration systems, operated by a registry authorised by the BACEN. The new regulation will also impose thresholds on the use of collateral over receivables from payment instruments.

With Circular No. 3,925/2018, which amended the Annex to Circular No. 3,682/2013, the BACEN addresses the provision of payment services within the framework of the arrangements of the SPB, establishing guidelines and standards these service providers need to abide by.

Furthermore, in line with the ongoing technological revolution, the BACEN published Circular No. 3,985/2020, defining the components of the instant payment system (SPI) infrastructure and establishing the participation of financial institutions and of payment institutions under the SPI, and Circular Letter No. 4,006/2020, setting out the form of registration of participants for the process of adhering to the instant payments system (PIX) – and the SPI. This is an important step taken by the BACEN with the aim of implementing an instant payment ecosystem in Brazil. By creating the SPI, the BACEN intends to foster the creation of an infrastructure that will allow people and companies to transfer money at any time, using more accessible payment mechanisms, such as QR codes in cell phones. This type of transfer tends to be more practical than those currently used, such as the available electronic transfer (TED) and credit order document (DOC), as it allows for instant transfer, does not require an intermediary and has lower costs. The BACEN itself will operate and coordinate the PIX. This infrastructure coordinates the relationship between service providers and instant payments.

Financial institutions with more than 500,000 active customers are now required to participate in the instant payment infrastructure and, consequently, of SPI, in order to settle instant payment transactions whenever they involve a transfer between instant payment accounts from different SPI participants. On the other hand, participation in the SPI is optional for entities that provide clearing and settlement services exclusively for the purpose of settling private liquidity supply operations carried out among SPI participants within the instant payment infrastructure.

The SPI provides for two forms of participation: direct and indirect. The first involves a direct connection of the participant institution to the SPI. Institutions that do not hold an operating permit from the BACEN are not allowed to participate in the direct form. The indirect participation form applies to institutions that do not hold a direct connection to the SPI and that do not have an SPI account. These institutions will operate through an intermediary, which must be a direct participant of the SPI infrastructure and will be responsible for registering and settling the operation entered under the SPI. Commercial banks, multiple banks with commercial portfolios, clearing and settlement service providers, among others, are not allowed to participate indirectly in the SPI.

The new rule is a step forward in BACEN’s initiative of establishing an SPI in Brazil, following the Bulletin No. 32,927 of 21 December 2018, in which the authority recognised the validity of instant payments and addressed the fundamental requirements for its environment within the Brazilian payment system regulatory framework. The implementation of the instant payments ecosystem in Brazil is expected to happen in November 2020. This model is favourable to the emergence of fintechs whose purpose is the development of innovative solutions to ease payment transactions. As announced by
the BACEN, fintechs will be able to act as payment institutions, supplying customers with payment accounts, or as payment initiation service providers. They may also offer other services such as insurance, credit, investments and tax payments, among others, fostering the development of innovative and competitive models and allowing for the reduction of social costs related to the use of paper-based instruments. The measures enable the inclusion of new players in the financial market, which is of extreme significance in a country with high rates of banking concentration such as Brazil.

Finally, there are currently no rules obliging institutions to make client or product data accessible to third parties. They are allowed to share with other financial institutions some information that can make the settling and clearing of payments faster, safer or more efficient. Nevertheless, this process must observe the applicable legal limits, as the Brazilian Federal Constitution (and specific laws such as the Supplementary Law No. 105/01) protects and assures the inviolability of banking secrecy, in most cases. With respect to clients’ personal data, under the LGPD, the process shall also be grounded on one of the legal bases provided for in the law. In this sense, possible legal bases that could be used to justify sharing are the consent of clients, the protection of credit and the legitimate interest of the financial institution. As already mentioned, the LGPD is still not effective, so the exact content and limits of the legal bases above are yet to be tested by Brazilian courts and further regulated by the Brazilian Data Protection Authority, which, as detailed in Section V below, was created by the LGPD, but will only initiate activities when the LGPD comes into force.

iv Marketplaces

A marketplace is a platform that connects buyers and sellers of goods or services with each other, providing an infrastructure with the purpose of facilitating a transaction. They are used in some business models as payment settlers to the extent that they receive the full amount paid by the customer and then pass the paid value on to sellers, which are their business partners, upon remuneration. In this kind of operation, marketplaces play the role of sub-accreditors, also called sub-acquirers or payment facilitators.

BACEN Circular No. 3.886/2018, which modifies Circular No. 3.682/2013, defines the role of the sub-accreditors and how they interact with payment arrangement providers. It also defines objective criteria for requiring the participation of sub-accreditors in a centralised settlement system in a single grid, which is also regulated by Circular Letter No. 3.872/2018. Circular No. 3.886/2018 categorises sub-accreditors that facilitate the acceptance of a payment instrument by the recipient, without being part of the transaction as a creditor, thus being the link between the end user and the accreditors, as participants in the payment arrangement infrastructure.

Moreover, the Circular determines that the intermediation of payments under the sub-accreditor model, which might include marketplaces, must comply with the payment arrangement infrastructure regulatory framework. Not all marketplaces are considered sub-accreditors. In cases where the transaction is carried out directly between the payer and the marketplace’s business partner, the marketplace will not be considered a sub-accreditor. In these cases, the seller itself will be the end user receiving the transaction payment.

Sub-accreditors are obliged to participate in the centralised settlement system. The centralised settlement system involves the centralisation of settlement of transactions.
performed by the payment arrangements that integrate the SPB in one neutral clearing and settlement service provider, defined by the institutions instituting those payment arrangements. The current clearing and settlement service provider is the Interbank Payment Chamber.

The marketplace participation in the centralised settlement system is mandatory, regardless of the volume of the transactions, if the sub-accreditor is the recipient of the flows relating to transaction in payment arrangements subject to centralised settlement. Nonetheless, the participation is optional if the marketplace acts as a payer to end users who receive flows related to transactions in payment arrangements subject to centralised settlement, and the volume of the operations accumulated in the last 12 months is lower than 500 million Brazilian reais. Brazilian legislation does not provide for special rules relating to digital or cryptoassets in marketplaces.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

There is no specific regulation in Brazil for blockchain technology. In fact, considering Brazil as a civil law jurisdiction, it would be necessary to modify a large number of laws, rules and other types of regulations to include legal provisions for all the currency and non-currency applications of such technology. Therefore, the Brazilian law does not recognise or establish a concept for blockchain or any of its applications, including cryptocurrencies.

Yet some financial authorities from Brazil have issued documents regarding cryptocurrencies and initial coin offerings (ICOs). Though not enforceable like laws, they are a good demonstration of how governmental agencies tend to define such assets.

Firstly, the BACEN stated that cryptocurrencies are not coins and cannot be equated with ‘electronic coins’, already defined in law as the virtual representation of fiat money. In Bulletin No. 31.379 from 16 November 2017, the entity issued an alert about the risk of operations involving cryptocurrencies and still remarked that such operations are subject to exchange rules and taxes on transactions referred in foreign currencies. The authority also conducts some tests regarding different possibilities of blockchain technology applications, such as an alternative system for transactions settlement and identity management.15

The CVM, in its competence regulating the securities market, published a note containing its perceptions about ICOs. The authority remembered that the law provides a description for the concept of security and the characteristics that can frame any asset into this concept. If a token give its owner any right as described in the law,16 it may be considered a security and the capital market regulations will apply to its offering, distribution and other transactions. Consequently, besides the laws suitable to securities, CVM Rules No. 400 (public offerings), No. 476 (limited efforts public offerings), No. 588 (crowdfunding) and others regarding securities operations need to be observed during an ICO process, and it does not matter if the issuer is Brazilian or foreigner. The CVM also stated that investment funds

---


16 Any title or collective investment scheme that generates the right to participation, partnership or remuneration, which income is originated in the effort of entrepreneurs or third parties, including those resultant from rendering of services, as described in Article 2, IX, Law No. 9.385/1976.
cannot perform direct cryptoassets operations in Brazil. However, in September 2018, the regulator authorised indirect investment in cryptoassets through, for instance, the acquisition of quotas of funds and derivatives, among other assets traded in third jurisdictions, provided that they are admitted as being regulated in those markets.

Finally, the Revenue Service determined that taxpayers must declare any gain obtained from transactions involving ‘virtual coins’ such as Bitcoin and other cryptoassets. If the operation is of an amount higher than 35,000 Brazilian reais, the individual must pay 15 per cent over the earnings as income tax.

VI OTHER NEW BUSINESS MODELS

Self-executing contracts, also known as ‘smart contracts’, are important deployments in the context of Blockchain technology. Therefore, since there is no specific regulation for technological applications of this nature, smart contracts are not yet foreseen in Brazilian law and may face questions regarding their legality, enforceability, validity and other characteristics necessary for contracts. However, they are not prohibited and if the basic contractual requirements are fulfilled, in specific cases smart contracts may be entered into in the same way as regular contracts.

As for the automated investment operations, it is necessary to distinguish two important professionals: the consultants – authorised only to advise investors, without managing funds of third parties – and portfolio managers (asset management) – who can make investments on behalf of third parties. For both, there is a legal provision for the use of algorithms and automated systems, whose source code must be delivered to the CVM and that do not exempt professionals from any responsibility in the provision of services. All agents are subject to securities market regulation, including third-party websites that provide or compare information about financial products.

If a sole investor wants to perform operations using automated algorithms like trading bots, they may execute orders before brokers using such systems. To do that, it is imperative that they comply with the rules established by the exchange itself and, mainly, securities regulation. Caution is needed by a bot user in order to avoid market manipulation and illegal practices such layering and spoofing, all of which are forbidden by the authorities; if this happens, the user will be responsible for any illegal act the system performs.

Some new business models shown by specific companies that are very relevant in the market have gained attention in recent years. The credit card operator ‘Nubank’ is particularly successful in Brazil. Their business models provide innovative approaches to traditional services, and sometimes regulatory discussions may directly impact their activities. In 2018, Nubank sold 5 per cent of its capital to the Chinese-based multinational investment holding TenCent, in exchange for a contribution of capital of approximately US$200 million. This makes Nubank one of the most valuable start-ups in Latin America, and one more LatAm unicorn.

PagSeguro Digital and Stone Pagamentos also experienced an astonishing capital growth in 2018, despite analysts alerting that the euphoric cycle of the American stock exchanges has ended. PagSeguro raised approximately US$ 2.27 billion in its initial public offering on the New York Stock Exchange, while Stone Pagamentos raised US$1.2 billion in the electronic Stock Exchange Nasdaq.

17 See Article 15, CVM Rule No. 505/2011.
Another good example is Geru Tecnologia e Serviços SA (Geru), an online lending platform. Geru Credit Rights Investment Fund (FIDC) is a fund structured as a closed condominium. Its portfolio of rights will be composed of bank credit notes, representing loans granted to debtors via Geru’s online platform. In August 2019, the fund received a Standard & Poor’s rating. Currently, the company is the only Brazilian lending fintech that has been rated by one of the three largest risk assessment agencies in the world. Creditas is also a successful case worth mentioning. Creditas is an online secured loan platform, which in August 2019 received a contribution of US$231 million from SoftBank Vision Fund and SoftBank Group Corp.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Generally, software in Brazil is protected by copyright law. Briefly, this means that source codes are equated to authorship works such as literary or artistic works, and it is not necessary to register it with the authorities to ensure protection. Therefore, any ownership dispute may be solved with proof of authorship. Nevertheless, it is possible to register the source code with the entity responsible for the registration and management of industrial property in the country – the National Institute for Industrial Property.

There are some cases in which patents can be issued regarding software and computer programs. This happens if it fills the requirements of characterisation of an industrial creation (a process or product associated with the process); thus, if the solution implemented by a computer program solves a problem found in the art and scope a technical effect that does not only concern how the computer program is written, it may be considered an invention and would be patentable.

To verify whether a new financial technology includes an invention protected by patent rights, it is necessary to know if it fits the following basic requirements: novelty; inventive step; industrial application; and technical effect. Note that the first three criteria apply to all patents, while the latter concerns the patentability of computer programs or software. The novelty requirement is broadly met when creation did not exist and was invented, that is, it is entirely new. Meanwhile, inventive step means that the invention was not obvious or obvious from the state of the art (a legal term used for what already exists and is available to the public). Industrial application is the possibility of using or producing the creation in any type of industry.

The technical effect considers the practical effects achieved throughout the steps developed by the invention implemented by the computer program. The general rule is that in order to grant a patent registration for software, there must be practical application in addition to the patentability requirements. In short, the industrial creation implemented by software may be subject to protection by patent rights if:

a it solves a problem found in the technique; and
b it achieves a technical effect that does not only concern how the software is written.

It is important to note that the patent application process involves accurately describing the invention created. This precise description will be the one that is protected. In this sense, a new version of the same software would not be covered by the same patent protection.

18 See Law No. 9.606/98, that regulates intellectual property for computer programs.
In any case, to determine the immediate ownership of software or computer program developed by third parties even before any registration or patent, it is necessary to verify the relationship with the author or inventor. If the creator is an employee and thus contracted under employment relationships, the rule of thumb provided by law is that the employer owns the intellectual property of software and computer programs developed in the context of the employee's activities. The contract executed between the parties may determine different aspects, but in the case of omission, this is the general rule.

Regarding data protection, data privacy legislation is going through important modifications in Brazil: as mentioned, the LGPD, that regulates any treatment of personal data, by public and private entities, in the online and offline environments, using automated and non-automated means was enacted in August 2018. The Law was inspired by international guidelines, especially those provided by the EU General Data Protection Regulation, but will only come into force in August 2020.

Currently, there are several pieces of legislation in Brazil dealing with different scopes of privacy and data protection such as intimacy, private life, honour, image and secrecy of correspondence, bank operations and communications. Such pieces of legislation include the Federal Constitution, the Civil Code, the Consumer Protection and Defence Code, the Banking Secrecy Law, the Brazilian Internet Act and the Criminal Code. However, the LGPD is the first omnibus law in Brazil that deals specifically with personal data protection without limiting its applicability to certain categories of agents and subjects (e.g., consumers, employees, financial institutions) or types of treatment (e.g., operation in the online environment).

The LGPD set standards and establishes important definitions to Brazilian data privacy regulation, such as personal data, sensitive personal data, anonymised data, data controller and data processor, among others. It adds to the framework surrounding data processing, including compliance with a legal or regulatory obligation, the fulfilment of a contractual or legal obligation and the controller's legitimate interest, as well as determining the details on how the user's consent must be collected to legitimise personal data processing.

The LGPD also addresses international transfer of personal data, rules on liability, data breach and penalties related to the violation of data privacy rights. The effects of the LGPD extend to any treatment of personal data carried out in the Brazilian territory, any treatment of personal data collected in the Brazilian territory, or any treatment of personal data made with the purpose of offering or supplying goods or services to individuals located in the Brazilian territory.

The LGPD further provided for the creation of the Brazilian National Data Protection Authority (ANPD). The ANPD will initiate its activities when LGPD is effective. Among other things, the ANPD will have authority to supervise the application of the LGPD, prosecute data incidents and apply penalties in the administrative sphere, and to issue regulations about specific points of the LGPD (such as the approval of standard contractual clauses and the list of countries offering a level of data protection similar to Brazil for the purposes of international transfer of personal data, security standards, duties of data protection officers, etc.).

Note that there are still some points pending with respect to the ANPD that should be resolved before August 2020: the appointment of the chairman and the other four executive officers of the ANPD, as well as 23 out of the 25 members of the ANPD’s advisory board are yet to be appointed, and the procedural rules applicable to future administrative proceedings to be conducted by the ANPD (e.g., prosecution of data incidents) are also open questions.
8 YEAR IN REVIEW

From a data protection standpoint, the most important outcome will be the entry into force of the LGPD and the start of the ANPD’s activities. From August 2020, the provisions, concepts, standards and procedures set forth in the LGPD will start being tested, interpreted and further regulated by Brazilian courts and the ANPD.

As regards the activities of the BACEN, as mentioned above, Resolution No. 4,734/2019 and Circular No. 3,952/2019, while dealing with the use of payment arrangement receivables as collateral for credit transactions, make lending to smaller companies feasible while also introducing several modifications related to the register of receivables of credit and debit payment instruments. This will facilitate discount operations of receivables from payment arrangements and credit operation collateralised by these receivables entered between commercial establishments and different institutions.

One of the most important highlights of last year’s regulatory innovation was BACEN Circular No. 3,985/2020, defining the components of the SPI infrastructure and establishing the participation of financial institutions and of payment institutions under the SPI. The creation of the SPI is an important step forward in allowing people and companies to transfer money at any time, using more accessible payment mechanisms. The expectation is that the measure will improve the fintech environment, since they will be able to develop solutions to make payment transactions easier for payers and payees.

It is also worth mentioning that the BACEN, in its efforts to adapt its regulatory framework to the innovation environment, launched Public Consultation No. 73/2019, on 28 November 2019 in order to gather the market’s opinion on a draft resolution regulating open banking, which means the disclosure of the customer’s banking information by the financial institutions so that other service providers can also use this information upon the authorisation of the data holder. Open banking has the potential to increase competition within the financial sector. The Consultation was open until 31 January 2020. Following the measure, on 3 March 2020, the BACEN published Ordinance No. 107,101, in which it created a working group with the task of proposing a structure responsible for the governance of the implementation of open banking in Brazil. New regulatory measures on the matter are expected soon.

IX OUTLOOK AND CONCLUSIONS

The volume of fintechs operating in the Brazilian market increased from 453 companies to 604 between August 2018 and June 2019, representing an increase of 33 per cent, which means that this is a growing sector with a lot of potential. The main objectives of recent regulations were to guarantee greater legal certainty, safety and confidence to the market while fostering competition between financial institutions. The authorities are showing cooperative behaviour, acting together to produce norms that could affect the market.

They are also combining efforts with the private sector, especially fintech players. Working together, the regulation may boost the use of technology applications that modernise and make financial services more efficient.

---

It is important to ensure adequate levels of safety without the creation of unnecessary regulations that could suppress the activity of companies whose products and services benefit the market; innovation is a powerful tool to promote the financial inclusion of citizens, and designing a legal framework to boost the creation of new technologies is a very important step in the development of the Brazilian society and economy.
Chapter 5

BRITISH VIRGIN ISLANDS

Ian Montgomery

I OVERVIEW

For the first six months of 2018, the British Virgin Islands (BVI) was the top market by volume, as indicated by CoinShares Research CryptoReport: H2 2018 (the Report), narrowly beating out the United States, and making it a substantial jurisdiction when it comes to cryptocurrency. The report was based on 14 of the largest cryptocurrency exchanges. This may be surprising to some; however, the BVI has always been a leading corporate domicile, with forward-looking legislation supported by a legion of skilled professionals based in the main financial centres around the globe.

As set out in the Report, such charting of jurisdictions is an indicator of the perceived legal, regulatory or other government-imposed risk of using certain jurisdictions. Clearly, the BVI is making its place as one of the preferred jurisdictions when looking to establish an enterprise in the fintech, blockchain or digital asset space.

II REGULATION

i Licensing and marketing

Financial services commission

The Financial Services Commission Act 2001 established the British Virgin Islands Financial Services Commission (FSC) as an autonomous regulatory authority responsible for the regulation, supervision and inspection of all financial services in and from within the BVI.

Regulated activities that are considered financial services include: insurance, banking, fiduciary services, trustee business, company management, investment business and insolvency services, as well as the registration of companies, limited partnerships and intellectual property.

While there is no specific regulation relating to fintech, the most likely FSC-regulated activities to be relevant to financial technology businesses are securities investment business, money services business and mutual funds business.

We have set out the basic legislation and principles below, but note that each particular case relies heavily on the specific facts that will be determinant of whether regulation may apply and if so, whether any exemption are available.

Additionally, as financial services regulator, the FSC is responsible for:

a promoting understanding of the financial system and its products;

---

1 Ian Montgomery is a managing partner at Collas Crill.
b policing regulated activities with a view to reducing financial crime; and
c preventing market abuse.

Investment business

Generally, the statute with the most relevance is the Securities and Investment Business (Amendment) Act 2019 (SIBA). SIBA regulates investment business in the BVI and effectively prohibits anyone from carrying on investment business of any kind in or from within the BVI unless that person holds the relevant licence. Alternatively, the person is excluded from requiring a licence or the activity itself is an excluded activity under SIBA.

For the purposes of SIBA, where the activity is carried on by a company incorporated in the BVI, if that company is carrying on investment business, even if the activity takes place entirely outside the BVI, the activity is deemed to be carried on in or from within the BVI, and the statute will apply.

Generally, a person will be engaging in investment business if that person carries out, by way of business, any of the following (among others):

a dealing in investments:
• buying, selling, subscribing for or underwriting investments as an agent; or
• buying, selling, subscribing for or underwriting investments as principal where the person (1) holds himself or herself out as willing, as principal, to enter into transactions of that kind at prices determined by him or her generally and continuously rather than in respect of each particular transaction; (2) holds himself or herself out as engaging in the business of underwriting investments of the kind to which the transaction relates; (3) holds himself or herself out as engaging, as a market maker or dealer, in the business of buying investments of the kind to which the transaction relates with a view to selling them; or (4) regularly solicits members of the public with the purpose of inducing them, whether as principals or agents, to buy, sell, subscribe for or underwrite investments and the transaction is, or is to be entered into, as a result of such person having solicited members of the public in that manner;

b arranging deals in securities: making arrangements with a view to (1) another person (whether as a principal or an agent) buying, selling, subscribing for or underwriting a particular investment, being arrangements which bring about, or would bring about, the transaction in question; or (2) a person who participates in the arrangements buying, selling, subscribing for or underwriting investments;

c managing investments:
• managing investments belonging to another person in circumstances involving the exercise of discretion (other than as manager of a mutual fund); or
• acting as manager of a mutual fund;

d providing investment advice:
• advising a person on investments (other than as the investment adviser of a mutual fund) where the advice is given to the person in his or her capacity as an investor or potential investor, or in his or her capacity as agent for an investor or a potential investor; and concerns the merits of the investor, or a potential investor, doing any of the following (whether as principal or agent): (1) buying, selling, subscribing for or underwriting a particular investment; or (2) exercising any right conferred by an investment to buy, sell, subscribe for, underwrite or convert an investment; and

e acting as the investment adviser of a mutual fund.
All of the above activities relate to or somehow involve an ‘investment’. Under SIBA, ‘investment’ means an asset, right or interest specified in Schedule 1.

The use of the word ‘means’ in the definition above requires that the investment must be listed in Schedule 1. There is no discretion or flexibility for the regulator to otherwise classify something as an investment unless it is in Schedule 1.

Investment is defined in Schedule 1 to SIBA as including shares, interests in a partnership or fund interests; debentures; instruments giving entitlement to shares, interests or debentures; certificates representing investments; options; futures; contracts for differences; and long-term insurance contracts. Essentially, financial instruments.

To the extent that any proposed activity touches on the concept of investment, as defined in SIBA, it is very likely that the licensing requirements under SIBA will apply.

**Financing and money services business**

Under the Financing and Money Services Act, ‘money services business’ is defined as the business of providing any of the following services:

- the dispensing of money, the facilitation of deposits, payments, transfer of money or the reporting of account information via automated teller machines;
- transmission of money in any form, including electronic money, mobile money or payments of money;
- cheque-cashing services;
- currency exchange services; and
- the issuance, sale or redemption or money orders or travellers’ cheques.

Under the BVI Interpretation Act, a reference to money in an enactment is a reference to the currency that is legal tender in the BVI, which means United States dollars. There is presently no recognition of virtual currencies (VC) in the BVI as being equivalent to fiat currency. As such, any reference in BVI legislation to ‘currency’ or ‘money’ will be interpreted as legal tender and will exclude VC.

Under the Financial Services and Markets Authority (FMSA), ‘financing business’ has recently been amended to include activities governed by a Class F licence, which are businesses engaged in international financing and lending in the peer-to-peer (P2P) fintech market, including peer-to-business (P2B) and business-to-business (B2B) markets.

To the extent that a financial technology business plans to engage in financing business or money services business, they would first need to apply for and receive the relevant licence under FMSA.

**Mutual funds**

While not usual for traditional fintech business, if an issuer offers coins or tokens with certain attributes, in particular that they are redeemable, then operators would need to consider whether there is a need to comply with the provisions of SIBA and the Mutual Fund Regulations.

SIBA covers mutual funds in Part III. Section 40 of SIBA defines ‘mutual fund’ as a company or any other body, a partnership or a unit trust that is incorporated, formed or organised, whether under the laws of the Virgin Islands or the laws of any other country that:

- collects and pools investor funds for the purpose of collective investment; and
issues fund interests that entitle the holder to receive on demand or within a specified period after demand an amount computed by reference to the value of a proportionate interest in the whole or in a part of the net assets of the company or other body, partnership or unit trust, as the case may be.

In our experience, it is not unusual for a fintech company to issue a redeemable token or coin. Such a company ought to take specific advice as to whether they will be regarded as a mutual fund and would be required to comply with SIBA.

**Public offering in the British Virgin Islands**

For completeness, Part II of SIBA deals with issuing securities to the public in BVI and prospectus requirements; however, Part II is not yet in force and it is not anticipated that it will come into force any time soon.

**ii Cross-border issues**

The BVI does not have a passporting regime specifically designated for regulated or licensed fintech entities to carry on business in the BVI.

Licensees under SIBA or other licensing legislation that have physical operations in the BVI are usually exempted from the requirement to obtain a licence under the Business, Professions and Trade Licences Act (BPTL). Where a business has a physical operation in the BVI but is not required to be licensed under other legislation, the catch-all licensing statute for business undertaken in the BVI is the BPTL.

BPTL is an older statute and the process for licensing is not as developed as it is under the financial services legislation. There is no specific licence for fintech activity and it is likely that the activity would fall under general commercial activity. The licensing process is straightforward and requires the submission of a simple application form that includes the details of the proposed business and financing. Applications can then be disapproved or approved subject to such terms and conditions as may be established, and the deposit of such sum of money as may be determined where the applicant is not located in the BVI. There are no time limits set out.

**III DIGITAL IDENTITY AND ONBOARDING**

The Electronic Transactions Act 2001 (ETA) should be considered when preparing and accepting the terms and conditions or purchase agreements relating to a coin or token offering or any other electronic transaction where offer and acceptance is entirely electronic. The ETA generally provides that information, documents and contracts (or any provision thereof) shall not be denied legal effect, validity or enforceability solely because they are in electronic form. Evidence of a contract (or provision thereof) shall not be denied admissibility solely because it is in electronic form, and electronic signatures are also expressly permitted. The ETA provides flexibility for transactional technologies without the requirement for further statute to be adopted. The ETA also provides a framework for the use of electronic signatures.
IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i Crowdfunding
The recent amendments to the FMSA appear designed to cover crowdfunding, and a Class F licence under FMSA would be required to the extent that the activity constitutes P2P, P2B or B2B lending or finance.

ii Collective investment schemes
As noted above, mutual funds are regulated by the FSC under SIBA and the Mutual Fund Regulations 2010. Closed-ended funds are not required to be registered, although other regulatory aspects (such as anti-money laundering/combating the financing of terrorism (AML/CFT) regulations) will still apply.

While there are three types of funds set out under the SIBA – public funds, private funds and professional funds – private and professional funds are by far the most popular.

A private fund is a fund whose constitutional documents specify that either:

- it will have no more than 50 investors; or
- the making of an invitation to subscribe for interests is to be made on a private basis; in other words, the invitation is made:
  - to specified persons (however described) and is not calculated to result in shares becoming available to other persons or to a large number of investors; or
  - by reason of a private or business connection between the person making the invitation and the investor.

A professional fund is a fund that is only available to professional investors (i.e., persons (1) whose ordinary business involves, whether for its own account or the account of others, the acquisition or disposal of property of the same kind as a substantial part of the property of the fund; or (2) whose net worth (whether individually or jointly with his or her spouse) exceeds US$1 million and who consents to being treated as a professional investor). A professional investor’s initial investment must be at least US$100,000 or its equivalent in another currency.

Both a private fund and a professional fund are very similar from a regulatory and cost perspective. However, a professional fund can prove useful as it may carry on business for up to 21 days prior to being recognised by the FSC, provided that the application for recognition is submitted to the FSC within 14 days of the launch of the fund.

The recognition or registration procedure for funds with the FSC is relatively straightforward, requiring the submission of:

- evidence of the formation of the entity (i.e., copies of the certificate of incorporation and memorandum and articles of association for a company);
- a completed application form and offering document; and
- evidence of the type of fund, for instance, an extract of the subscription agreement showing the professional investor declaration referred to above.

Any private or professional fund that intends to make an offer of its interests or shares must include the prescribed investment warning in a prominent place in the offering document. The subscription agreements must include a written acknowledgement from any new investor that it has received, understood and accepted the investment warning. Professional funds should also include statements in their constitutional documents as to its professional fund status.
A private or professional fund must appoint a manager, an administrator and a custodian (although application may be made to the FSC to exempt a fund from appointing a manager or custodian). Such funds are also required to have two directors, but they need not be resident in BVI and appoint a local authorised representative who will accept service on behalf of the fund in the BVI.

Recently, two newer categories of funds have been introduced and are proving very popular in the start-up and initial fundraising stages. Incubator funds and approved funds were introduced in the BVI under the Securities and Investment Business (Incubator and Approved Funds) Regulations 2015.

An incubator fund has a minimum investment requirement of US$20,000, a cap on net assets of US$20 million and limit of 20 investors. An incubator fund does not need to appoint a custodian or investment manager.

An approved fund has a net assets cap of US$100 million and no more than 20 investors are permitted, but with no minimum investment criteria. An approved fund may operate without appointing a custodian or investment manager, but will need an administrator.

An incubator fund or approved fund can commence business two days from the date of receipt of a completed application by the FSC. An incubator fund has a limited life of two years, which can be extended for up to 12 months. An approved fund has no such limits. An incubator fund can convert to an approved fund, a private or professional fund, or may wind up at the end of its term.

Corporate mutual funds are the most common vehicle and are managed by their directors of which there should be a minimum of two. However, the day-to-day operations of a mutual fund will normally be delegated to other specialist professionals.

**Payment services**

As noted previously, payment services would fall under the FMSA. Anyone seeking to operate a payment service ought to consider the obligations arising under the FMSA.

**V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS**

The BVI has one of the largest cryptocurrency markets in the world, and while there are no initial coin offerings (ICOs) or blockchain-specific rules or guidance, existing legislation is sufficiently flexible to support the continuing number of ICOs launching from the BVI. At present, it is an exercise in applying the existing legislation and regulatory regime described elsewhere in this chapter to each specific situation. In most instances, ICOs would not usually fall within the definition of investment under SIBA, and therefore there should be no need for the issuer to hold an investment business licence. However, there is still a concern that, depending on how they are structured, certain forms of ICOs may fall within the definition of investment and therefore the terms of each need to be carefully considered.

**VI INTELLECTUAL PROPERTY AND DATA PROTECTION**

The BVI Trademarks Act is the legislation governing the protection of intellectual property in the BVI. A fintech can utilise the process provided via this Act to protect their intellectual property rights.

At present, the BVI has not enacted legislation to regulate data protection. However, it is expected that the BVI will follow international standards in this area and adopt legislation
that reflects globally recognised standards. Service providers in the BVI currently operate under common law and contractual duties of confidentiality and privacy. These duties are subject to exceptions most notably in the area of anti-money laundering. Additionally, BVI regulated service provider may have similar duties imposed on them under applicable legislation.

The General Data Protection Regulation (GDPR) that which came into force on 25 May 2018 primarily gives EU citizens control over their personal data, including its collection, processing and storage – wherever it is held, processed or transferred.

However, the GDPR applies to the processing of personal data by a controller or processor established in the EU or outside the EU if their data processing activities relate to the offering of goods or services to individuals in the EU or to the monitoring of such individual’s behaviour.

While most businesses in the BVI should not directly be affected, those that collect the personal information of EU Citizens, or those marketing in the EU may be in scope and thus subject to the GDPR. In addition, other service providers may also be caught by the wide ranging scope of the GDPR, and accordingly, investment funds will need to be vigilant and ensure that any delegation of the processing of data by such service provider is being done in compliance with the GDPR.

VII YEAR IN REVIEW

The past years have seen many developments. For instance, the launch of the microbusiness company (MBC), which is aimed at small, non-financial sector businesses anywhere in the world. MBCs are simpler to set up and operate and have lower registration and annual fees. One of the most exciting aspects of the MBC is the use by the FSC of an online platform that enables AML checks and MBC formation to be carried out online.

Building on the use of an online platform, the AML Code of Practice has been amended to allow AML checks to be carried out using the latest electronic innovations, which should improve and speed up know-your-customer processes in the BVI.

The new Limited Partnership Act 2017 came into force, which incorporates the best practices for limited partnerships from other jurisdictions. It is expected that this will dramatically increase the use of BVI limited partnership structures. Similarly, BVI segregated portfolio companies are no longer restricted in their use to funds and insurance companies, opening the ability to use these companies in innovative ways.

Additionally, there have been amendments to the FMSA described above to facilitate P2P, P2B and B2B financing and lending.

VIII OUTLOOK AND CONCLUSIONS

The BVI remains committed to introducing measures and creating an environment where businesses involved in fintech, blockchain and artificial intelligence can thrive. The BVI remains at the forefront of international corporate structuring for cross-border transactions and investing, and provides market-leading expertise and products in areas such as banking and finance. The BVI is building on these strengths as it readies itself to move forward into the digital age.
Chapter 6

CAYMAN ISLANDS

Alan de Saram, Natalie Bell, Aoife Madden, Laura Smalley and Dawn Major

I OVERVIEW

With a long history of embracing financial innovation and providing a home for entrepreneurial technology companies, the Cayman Islands has experienced organic development as a financial technology hub. The Islands’ regulator, the Cayman Islands Monetary Authority (CIMA), has allowed the sector to flourish alongside the country’s existing legislative framework. CIMA, along with the Cayman Islands government, has pledged to introduce new legislation to encourage further development including the implementation of legislation which will address the need to provide additional regulatory measures for certain virtual asset activities in the Cayman Islands, a regulatory sandbox regime for digital assets and other innovative financial technologies (the virtual assets laws).

II REGULATION

i Licensing and marketing

Financial services business

CIMA oversees the regulation of financial services on the island. CIMA was formed by statute and is operated pursuant to the Monetary Authority Law (the 2020 Revision). Its mission is to protect and enhance the reputation of the Cayman Islands as an international financial centre by (1) utilising a team of highly skilled professionals and current technology; (2) carrying out appropriate, effective and efficient supervision and regulation in accordance with relevant international standards; and (3) maintaining a stable currency, including the prudent management of the currency reserve.

Anyone wishing to conduct banking, investment fund, securities, trust, money services, insurance or companies management business in or from the Cayman Islands will need to register with, be licensed by or seek an exemption from CIMA. CIMA prepares and issues a framework of conduct policies, statements of guidance and rules and forms that set out both broad principles and detailed requirements to which relevant entities must adhere.

While there is not yet any specific regulation relating to fintech, the most likely of CIMA-regulated business areas to be relevant to financial technology businesses are securities investment business, money services business and investment funds business. We have set out the basic definitions below. Depending on the specific facts, there are various exemptions.
available that may allow a person to be exempt from the requirement to obtain licensing from CIMA or to approach regulation in a different manner (e.g., registration rather than licensing).

**Securities investment business**

A person carries on securities investment business if that person is:

*a* dealing in securities:

- buying, selling, subscribing for or underwriting securities as an agent; or
- buying, selling, subscribing for or underwriting securities as principal where the person entering into that transaction (1) holds themselves out as willing, as principal, to buy, sell or subscribe for securities of the kind to which the transaction relates at prices determined by that person generally and continuously rather than in respect of each particular transaction; (2) holds themselves out as engaging in the business of underwriting securities of the kind to which the transaction relates; or (3) regularly solicits members of the public with the purpose of inducing them, as principals or agents, to buy, sell, subscribe for or underwrite securities and such transaction is entered into as a result of such person having solicited members of the public in that manner;

*b* arranging deals in securities. Making arrangements with a view to:

- another person (whether as a principal or an agent) buying, selling, subscribing for or underwriting securities; or
- a person who participates in the arrangements buying, selling, subscribing for or underwriting securities;

*c* managing securities. Managing securities belonging to another person in circumstances involving the exercise of discretion;

*d* advising on securities. Advising a person on securities if the advice is:

- given to the person in that person's capacity as an investor or potential investor or in that person's capacity as agent for an investor or a potential investor; and
- advice on the merits of that person's doing any of the following (whether as principal or agent): (1) buying, selling, subscribing for or underwriting a particular security; or (2) exercising any right conferred by a security to buy, sell, subscribe for or underwrite a security;

*e* managing an EU connected fund;

*f* marketing an EU connected fund; and

*g* acting as depositary of an EU connected fund.

The definition of ‘securities’ is set out in Schedule 1 to the Securities Investment Business Law (2020 Revision) (SIBL), and includes shares, instruments creating or acknowledging indebtedness, instruments giving entitlement to securities, certificates representing securities, options, futures and contracts for differences. As part of Cayman’s initiative to introduce additional regulatory measures for virtual assets activities, the definition of ‘securities’ may be amended in the future to include ‘virtual assets’. For a discussion of coins and tokens as securities, see Section V.

A person carrying on securities investment business may operate without applying for a licence and may simply register with CIMA in certain circumstances – typically where the company’s clients are limited strictly to high net worth and sophisticated persons.
The SIBL offers an exclusion for entities that are carrying on securities investment business (e.g., arranging deals in primary issue of securities) on their own behalf. That said, a Cayman Islands company that is the promoter, arranger or broker of securities of a separate issuer is likely to be caught by the definition and subject to the licensing requirement.

**Money services business**

Under the Money Services Law (the 2020 Revision) (MSBL), a person carries on money services business if the person carries on the principal business of any or all of the following:

- money transmission;
- cheque cashing;
- currency exchange;
- the issuance, sale or redemption of money orders or traveller’s cheques; and
- such other services as the Cabinet may specify by notice published in the Gazette.

**Currency exchange**

The third category of money services business, ‘currency exchange’, is generally taken to mean the business of exchanging one currency for another. There is ongoing debate as to whether virtual currencies and digital assets comprise currency, a commodity, goods or services. The provisions of the MSBL may need to be contemplated when exchange services in respect of a virtual currency or digital asset are going to be provided in or from within the Cayman Islands. Similarly, for a business that will offer a platform for exchange across digital currency pairs, or exchange from fiat-to-digital currency or vice versa, the MSBL will be important to consider.

To the extent that a financial technology business plans to engage in money service business, they would first need to apply for and receive a money services business licence from CIMA.

**Investment fund business**

While atypical for traditional fintech business, if an issuer offers coins or tokens with certain attributes, the operators would need to consider whether there is a need to comply with the provisions of the Mutual Funds Law (2020 Revision) (MFL) or the Private Funds Law 2020 (PFL).

The MFL applies to Cayman Islands entities, formed as collective investment schemes, that issue equities that are redeemable at the option of the holder (open-ended). The PFL, enacted in February 2020, applies to Cayman Islands entities formed as collective investment schemes that issue equities which are not redeemable at the option of the holder (closed-ended). In our experience, it is not unusual for a fintech company to issue a redeemable or non-redeemable token or coin. Such a company ought to take specific advice as to whether they will be regarded as a mutual fund or private fund, and as such will be required to comply with the MFL or the PFL.

**The Companies Law and offering of securities to the public in the Cayman Islands**

While not a CIMA-related issue, Section 175 of the Companies Law (the 2020 Revision) (the Companies Law) prohibits an exempted company incorporated in the Cayman Islands that is not listed on the Cayman Islands Stock Exchange from making any invitation to the public in the Cayman Islands to subscribe for any of its securities. A similar provision
relating to limited liability companies is contained in the Limited Liability Companies Law. The definition of ‘the public’ does not include an offering to other exempted companies and exempted limited partnerships. If a fintech issuer is doing a focused offering into the Cayman Islands and to its general population, this obligation might be triggered.

ii Cross-border issues
The Cayman Islands does not currently have a passporting regime specifically designated for regulated or licensed fintech entities to carry on business in the Cayman Islands.

Typically, in order to carry on business in the Cayman Islands on a domestic basis, a company will need to comply with a suite of domestic laws including the Local Companies (Control) Law (the 2019 Revision) (LCCL), the Trade and Business Licensing Law (the 2019 Revision) and, to the extent any foreign workers are employed, the Immigration (Transition) Law 2018.

In an attempt to make Cayman more ‘open for business’ at a local level and to ease barriers to entry with respect to businesses intending to have a presence in Cayman, Cayman Enterprise City has been set up in the Cayman Islands and benefits from generous concessions granted by the Cayman Islands government (including fast-tracked immigration processing and reduced annual fees), designed to incentivise businesses to set up and operate physical staffed offices in the Cayman Islands, provided that such business do not carry on activities which require licensing under certain laws and regulations of the Cayman Islands.

III DIGITAL IDENTITY AND ONBOARDING
The Electronic Transactions Law 2003 (ETL) should be considered when preparing and accepting the terms and conditions or purchase agreement relating to an SCO, STO or any other electronic transaction where offer and acceptance is entirely electronic. The ETL provides that information, documents and contracts (or any provision thereof) shall not be denied legal effect or validity solely because they are in electronic form. Evidence of a contract (or provision thereof) shall not be denied admissibility solely because it is in electronic form. Electronic signatures are also expressly permitted. The ETL provides flexibility for transactional technologies without the requirement for further statute to be adopted.

IV DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES
i Crowdfunding
CIMA has not adopted a formal position on crowdfunding. That said, to the extent a proposed crowdfunding project overlapped with any of the conventional business areas that require licensing, a proprietor ought to seek advice. In particular, the operator of a crowdfunding business would seek clarification of whether the SIBL, MFL or PFL would apply.

ii Collective investment schemes
As noted above, investment funds are regulated by CIMA under the MFL and PFL. All regulated funds must be audited by a firm of auditors approved by CIMA and located in the Cayman Islands (although there is no objection to the field work being done elsewhere). Prior to February 2020, closed-ended funds and open-ended funds with no more than 15 investors who, by majority, could appoint or remove the operators of the fund (Section 4(4) funds)
were not required to be registered, although other regulations such as anti-money laundering/combating the financing of terrorism (AML/CFT) still applied. As a result of certain EU and other international recommendations the Cayman Islands investment fund regime is now aligned with other jurisdictions. Closed-ended funds are regulated by the PFL and Section 4(4) funds are regulated by the MFL.

There are five main categories of regulated fund, given below.

**Registered mutual funds (MFL Section 4(3)) – open-ended**

Funds that require a minimum initial investment of at least US$100,000 (i.e., those targeted at institutional or sophisticated high net worth investors) or which are listed on an approved stock exchange may be registered on filing the following documentation with CIMA:

- a prospectus that properly describes the equity interest (i.e., shares) and contains the information necessary to enable a prospective investor to make an informed decision as to whether or not to subscribe;
- an application form;
- a letter of consent from the auditors and administrator (if applicable);
- an affidavit from the directors of the fund;
- evidence of incorporation or registration; and
- the prescribed registration fee and the initial administrative filing fee.

These funds are required to have their accounts audited annually and at least two natural persons, both registered with CIMA under the Directors Registration and Licensing Law 2014 (DRLL), as directors.

The majority of regulated funds in the Cayman Islands fall into this category. We have advised on the launch of regulated funds that invest in whole or in part in digital assets. There is no requirement that the administrator of a registered fund is resident in the Cayman Islands and the emphasis is on self-regulation. The fund must, however, have locally approved auditors.

**Administered mutual funds (MFL Section 4(1)(b)) – open-ended**

Funds, including those that permit a minimum initial investment of less than US$100,000, may be established by appointing a licensed mutual fund administrator to provide the principal office of the fund in the Cayman Islands. The administrator has primary regulatory responsibility for the administered fund and has a statutory duty to ensure that the fund is properly administered and that the promoters are of sound reputation. The administrator has a statutory obligation to notify CIMA if it knows or has reason to believe that a fund for which it provides the principal office is or is likely to become insolvent or is carrying on business in a manner that is or is likely to be prejudicial to its investors or creditors. The auditors have a similar statutory obligation as described above for registered funds. Similar documentation to that required for a registered fund must be filed with CIMA by the licensed administrator in respect of an administered fund and the prescribed fee paid.
Licensed mutual funds (MFL Section 4(1)(a)) – open-ended

Funds (typically retail funds) that are established and operated by large, well-known and reputable institutions may apply for a mutual fund licence. CIMA must be satisfied that the promoting institution is of sound reputation and that the fund will be properly administered by fit and proper persons with sufficient expertise before a licence will be granted. Such funds do not require a minimum initial investment by investors.

Registered mutual funds (MFL Section 4(4)) – open-ended

Funds carrying on business in or from the Cayman Islands that were previously exempt from CIMA regulation under Section 4(4) of the Mutual Funds Law by virtue of having no more than 15 investors who, by majority, can appoint or remove the operators of the fund must now register by doing the following:

- submitting an application form to CIMA;
- filing a prospectus or marketing materials or a summary of terms which comply with all applicable CIMA policies and rules;
- filing a letter of consent from the auditors (if available) and administrator (if applicable);
- filing evidence of incorporation or registration;
- filing a certified copy of their constitutive documents which specify that a majority of investors in number are capable of appointing or removing the operator of the fund; and
- payment of the prescribed registration fee.

A Section 4(4) fund will not be required to have a prescribed minimum initial investment amount. The Mutual Funds (Amendment) Law 2020 (the Amendment Law) provides that a Section 4(4) fund will be required to have its accounts audited annually and at least two natural persons, both registered under the DRLL as directors. The Amendment Law provides Section 4(4) funds (in existence at the time of its enactment or having been formed thereafter) with a transition period ending 7 August 2020 in which to comply. CIMA is expected to provide further guidance imminently.

Private funds (PFL Section 5) – closed-ended

The PFL applies to investment vehicles whose principal business is the offering and issuing to investors of its participating, non-redeemable (closed-ended) investment interests, the purpose or effect of which is the pooling of investor funds with the aim of spreading investment risks and enabling investors to receive profits or gains from such a vehicle’s investment activity, where (1) the holders of investment interests do not have day-to-day control over the vehicle’s investment activities; and (2) the investments are managed as a whole by or on behalf of the fund operator for reward based on the vehicle's assets, profits or gains. A closed-ended fund will be required to register with CIMA by doing the following:

- submitting an application form to CIMA;
- filing a prospectus or marketing materials or a summary of terms which comply with all applicable CIMA policies and rules;
- filing a letter of consent from the auditors and administrator (if applicable);
- filing evidence of incorporation or registration;
- filing a certified copy of their constitutive documents;
- filing a structure chart;
A registered private fund is expected to have its accounts audited annually, appoint a custodian (if necessary), appoint someone to monitor its cash flow and carry out frequent valuations of its assets. The PFL provides current and new closed-ended funds with a six-month transition period ending on 7 August 2020 in which to comply with the PFL. CIMA is expected to provide further guidance imminently.

Corporate investment funds are the most common vehicle and are managed by their directors of which there should be a minimum of two natural persons. However, the day-to-day operations of an investment fund will normally be delegated to other specialist professionals.

Directors of CIMA-regulated investment funds (along with companies registered as excluded persons under SIBL (each a ‘covered entity’) are required to be registered or licensed with CIMA under the Directors Registration and Licensing Law 2014 (DRLL). This requirement does not extend to directors of registered private funds.

The DRLL distinguishes between professional directors (being a natural person appointed as a director of 20 or more covered entities), corporate directors (being a body corporate appointed as a director of a covered entity) and registered directors (being individuals who are not professional directors). An individual acting as a director of an existing covered entity is required to be registered with CIMA.

Directors not already registered with CIMA under the DRLL must first register for a director account with CIMA via the CIMA Connect portal by providing details, including the name of the covered entity for which they are to act as director.

Regulated investment funds are required to file the following with CIMA on an annual basis:

- **prescribed fee to be paid by 15 January; and**
- **audited accounts to be filed within six months of the end of the financial year of the fund.**

Promoters and operators of regulated investment funds (i.e., directors, trustees or general partners, as the case may be) also have a statutory obligation to notify CIMA of (1) of any change that materially affects the information submitted to CIMA of which they are aware, and (2) any change in the details of its registered or principal office, within 21 days.

### iii Payment services and currency exchange

As noted above, payment services and digital currency exchange are likely to fall under the MSBL. Anyone seeking to operate a payment service or digital currency exchange ought to consider the obligations arising under the MSBL.

### V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS (ICOS)

CIMA has not, to date, issued formal guidance on the issuance and distribution of cryptocurrencies and initial coin offerings (ICOs) and token offerings, other than guidance issued to ‘virtual assets service providers’ on their AML/CFT obligations.
That said, any issuer or arranger of an offering of coins or tokens will need to determine whether the offer constitutes an offering of securities, as this may require a licence from CIMA.

The offering by a token issuer of its own token (notwithstanding the token may represent a security for the purposes of SIBL) is exempt from any licensing requirement. However, if there is (1) any offering of a security to the public in the Cayman Islands; (2) an offering of securities by a Cayman Islands company on behalf of a fintech issuer; or (3) a material carrying on of business in the Cayman Islands, the issuer should seek legal advice with respect to the applicable requirements of the LCCL, the Companies Law, immigration laws and SIBL.

VI INTELLECTUAL PROPERTY AND DATA PROTECTION

The Cayman Islands Intellectual Property Office is a division of the Cayman government’s General Registry Division, and allows for registration of trademarks, patents, copyrights and design rights. Since 2015, the Cayman Islands government has steadily introduced legislative measures with the aim of improving the rights and protections of holders of intellectual property developers and holders, and facilitating further IP-related business in the jurisdiction.

The Cayman Islands Data Protection Law 2017 (DPL) came into force on 30 September 2019 and regulates the processing of personal data in the Cayman Islands and by entities established in the Cayman Islands. The DPL, which applies to legal and natural persons, ensures that data controllers and data processors control and process personal data in line with internationally established data protection principles adopted around the world. The DPL provides data subjects with specific rights that protect how personal data is processed and controlled. The Office of the Ombudsman is the supervisory authority. A breach of the DPL can result in hefty fines and imprisonment.

VII ECONOMIC SUBSTANCE

The Cayman Islands government in an effort to meet its commitments as a member of the OECD’s global Base Erosion and Profit Shifting Inclusive Framework has enacted the International Tax Co-operation (Economic Substance) Law 2020 (ESL), which (albeit in a prior iteration of the law) came into force on 1 January 2019.

The ESL sets out requirements that relevant entities that carry on relevant activities must demonstrate that such entities have ‘economic substance’ (the ES test) in the Cayman Islands for each relevant activity that is being conducted. An investment fund, exempted limited partnership, domestic companies and entities that are tax resident outside the Cayman Islands are not relevant entities for the purpose of the ESL.

Banking business, distribution and service centre business, financing and leasing business, fund management business, headquarters business, holding company business, insurance business, intellectual property business, and shipping business are relevant activities under the ESL.

The requirements of the ES test are varied and depend on the relevant activity that is being conducted by the relevant entity. A relevant entity conducting a holding company business is subject to a reduced test which may be satisfied by simply engaging the services of its registered office providers. An entity conducting high-risk intellectual property business is
subjected to a more stringent test as it must rebut the presumption that it has not satisfied the ES test. Fintech industry participants will want to take a close look at their relevant activities to ensure compliance.

The Cayman Islands Tax Information Authority (TIA) is the supervisory authority that ensures compliance with the ESL. In addition to satisfying the ES test, all entities must notify the TIA as to whether it is conducting a relevant activity and whether it is a relevant entity. Relevant entities conducting a relevant activity must also submit an annual report to the TIA.

**VIII YEAR IN REVIEW**

The Cayman Islands had a number of developments in 2019, including further industry utilisation of Cayman Islands foundation companies, bolstering of anti-money laundering measures, and introduction of international tax cooperation (economic substance) laws.

Cayman Islands foundation companies have remained a favourite for issuers of SCOs, STOs and other tokens – particularly for the holding of any platform. Civil law foundations have, from time to time, been used by coin and token issues, either for tax or altruistic reasons. Cayman Islands foundation companies are unique in that they bear characteristics of both civil law foundations, in that they emulate some aspects of trusts, and companies, in that they have a separate legal personality and can take advantage of a settled body of company laws. A multitude of issuers and related industry groups have gravitated toward foundation companies as a flexible tool for either the issuer vehicle or a corporate governance vehicle for acting on the e-vote of designated coin and token holders.

As we hear from our clients and generally in the industry, Cayman Islands banks, as with many such financial institutions around the globe, are reluctant to open bank accounts for entities that will be exchanging digital assets for fiat currency (and vice versa). Concerns communicated include concern over AML/CFT aspects, pressure from correspondent banking partners or pressure from shareholders. We are hopeful that greater and broader understanding of the fintech industry and better and thoughtful regulation of the global industry will lead to a more welcoming environment for prospective banking clients.

**IX OUTLOOK AND CONCLUSIONS**

We believe that CIMA is keen to take a very practical and commercial approach to STOs, SCOs and fintech in general, in order to maintain Cayman's reputation as a leading finance centre. CIMA has not, as yet, issued any formal guidelines but we understand that CIMA will issue guidance in the future, which will be based on consultations with reputable participants in the blockchain industry. Drafts of the virtual assets laws are currently out with industry for consultation. CIMA's goal is to develop an effective and business-friendly fintech landscape, which also aligns with international standards as they continue to develop.

In common with most jurisdictions, increasing compliance with strengthened AML/CFT/KYC has been, and will continue to be, a significant addition to onboarding and operational aspects of doing business in the Cayman Islands. Indeed, CIMA has stated that
its primary concern with fintech offerings is the AML/CFT-related aspect.² Such concerns will most certainly make up a large part of the specific guidance once released, and may serve to give comfort to all fintech players and service providers (including banking institutions).

Because the Cayman Islands has a forward-looking regulator, combined with a legislative assembly that has introduced such helpful innovations as the Foundation Companies Law, Cayman Enterprise City and its successful Special Economic Zone Companies, the many fintech entrepreneurs which seek Cayman Islands as a jurisdiction for business look to be well served in the future.

I OVERVIEW

Since the publication of the second edition of The Financial Technology Law Review in 2019, the German fintech market has matured. It seems that a consolidation phase has been reached where the fintech market’s influence on the financial sector is of rather evolutionary nature. Although a ‘winner-takes-all’ phenomenon was recently observed in the fintech industry (attributed to increased competition and high acquisition costs), fintechs are expected to benefit from new business opportunities, especially in the field of artificial intelligence, big data and distributed ledger technology. It might also be perceived as an indication of a matured market that fintech companies have increasingly been integrated by banks and financial institutions into their value chains. The trend towards consolidation might further be accelerated by the current corona-virus pandemic, which is likely to result in tremendous challenges for all participants in the financial sector.

These developments, however, do not mean that the German fintech market has become stagnant. The opposite is true. Fintech-related topics have been frequently and intensively discussed in Germany not only by participants in the financial sector but also by politicians and regulatory authorities. The public interest caused by Facebook’s initiative to introduce Libra as a global virtual payment instrument backed by fiat currencies has certainly contributed to the momentum of the current developments. Particularly the question of whether the present legal framework gives sufficient leeway for the application of blockchain-based business models while simultaneously providing a sufficient level of protection for market participants has been the subject matter of such discussions. As a result, the German legislator recently introduced new statutory provisions according to which crypto values qualify as financial instruments for financial licencing purposes. Further, the crypto custody business was introduced as a new type of service, which is subject to a licence requirement under the German Banking Act (KWG).

1 Jens H Kunz is a partner at Noerr LLP.
4 See the English version of BaFin’s article: Evolutionary influence of fintechs on the financial sector: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2019/fa_bj_1911_Fintech_en.html (23 March 2020).
In recent years the activities in the field of policy and financial market regulation that have been sparked by the insight that digitalisation will fundamentally change the financial industry included the assignment of a study to get a better understanding of the fintech market in Germany, the formation of the FinTech Council by the German Federal Ministry of Economics that aims to enhance the dialogue among business, politics and academia as well as a joint paper of the German Federal Ministry of Finance and the German Federal Ministry of Justice and Consumer Protection concerning the regulatory framework for blockchain-based securities and crypto tokens aimed at fostering innovation and investor protection. Further, the German Federal Financial Supervisory Authority (BaFin) has published several statements, explanations and opinions, including the perspective of BaFin on topics such as big data and artificial intelligence, distributed ledger technologies as well as digitalisation and information security. The new statutory rules on crypto values and the crypto custody business as well as the plans of the German government concerning special rules for blockchain-based securities also indicate that the legislator has realised the need to provide legal certainty for innovative business models and services.

Generally, German legislator and BaFin apply the technology-neutral principle of ‘same business, same risk, same regulation’. This includes that neither the legislator nor BaFin has promulgated rules that privilege fintech companies compared to traditional players in the financial sector. Therefore, a ‘sandbox’ model that establishes an innovation space where fintech companies may test business models without tight regulation as established in the United Kingdom and in Switzerland has not been introduced in Germany yet.

Hence, BaFin attempts to find a balance between supervisory concerns and the start-up culture that often exists in fintech companies. As part of its efforts in this regard, BaFin provides fintech companies with information concerning supervisory issues on their website.

There is no special public funding instrument for fintech companies, but the German Ministry of Economics has set up the programme ‘INVEST’ to help start-ups raise venture capital. If business angels purchase shares of newly founded innovative companies and hold them for more than three years, 20 per cent of their original investment will be reimbursed by the state up to a limit of €100,000. To qualify for the programme, investors have to spend at least €10,000. Invested capital must not result from a third-party loan to the investor.

---

6 See German Federal Ministry of Finance (Bundesministerium der Finanzen), www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2017/03/2017-03-22-pm-fintech.html (23 March 2020).
8 See the English version of the related BaFin-website where BaFin gives a summary of its position on fintech related regulatory questions: https://www.bafin.de/EN/Aufsicht/FinTech/fintech_node_en.html (23 March 2020).
Furthermore, the business angel has to participate in the new company’s gains and losses. Investors must be natural persons living in the European Economic Area or must use special investment companies registered in Germany (e.g., the limited liability company, GmbH).

Generally speaking, German regulatory authorities and the government emphasise that they recognise the potential of fintech for public economic benefit, while the regulation still seems rather conservative when the traditional regulatory standards, which stem from the pre-digitalisation era, are applied. Nevertheless, the efforts of BaFin to support fintech companies by offering detailed legal information and by improving the communication channels, as well as recent legislative changes concerning the regulatory requirements for cryptoasset-related services, are evident.

II REGULATION

i Licensing and marketing

The general rules apply to licensing and marketing of fintech companies in Germany. Since there is no specific fintech licence available in Germany, the regulation of fintech companies depends ultimately on the business they carry out. This again results from the technology-neutral ‘same business, same risk, same rules’ approach. The entire array of licences and marketing restrictions may therefore become relevant for fintech business models.

In particular, the following types of licences have to be taken into account:

a) licence pursuant to Section 32 (1) Banking Act (KWG) for providing banking businesses within the meaning of Section 1(1)(2) KWG or financial services within the meaning of Section 1(1a)(2) KWG (including, since 1 January 2020, the crypto custody business within the meaning of Section 1(1a)(2) No. 6 KWG, which is of particular relevance for fintech companies);

b) licence pursuant to Section 10(1) Payments Services Supervisory Act (ZAG) for providing payment services or pursuant to Section 11 ZAG for the issuance of e-money;

c) licence pursuant to Section 20(1) Capital Investment Code (KAGB) or, less burdensome, the mere registration pursuant to Section 44(1) KAGB for offering collective asset/ funds management;

d) licence pursuant to Sections 34c, 34d and 34f Industrial Code (GewO) for the brokerage of loans, insurance contracts and certain financial products; and
e) licence pursuant to Section 8(1) Insurance Supervisory Act (VAG) for conducting insurance business.

In general a licence requirement is triggered if someone intends to provide in Germany commercially or on a scale which requires a commercially organised business undertaking one of the services listed in the comprehensive catalogues of regulated activities referred to above. Consequently, it needs to be carefully analysed whether a fintech business model falls within the scope of one or several of such regulated services.

Depending on the type of licence, different authorities might be competent to grant the relevant licence. Placing the competent authorities in a hierarchy, the European Central Bank (ECB) is at the top with its competence for granting licences for institutions that intend to carry out banking business that includes lending and deposit-taking business. Beneath the ECB, BaFin is the competent authority for institutions that intend to provide banking business except for lending and deposit taking, including investment services and other financial services, payment services, collective asset or funds management and insurance
business. The third level in the hierarchy would consist of the authorities which have been endowed under the German federal state laws with the competence to grant licences pursuant to the GewO.

All these types of licences may become relevant for fintech business models. This can be illustrated by the observation that the first ‘fintech banks’ were established in Germany holding a banking licence granted by ECB.

Both the requirements to obtain a licence under the German financial supervisory laws and subsequent ongoing legal requirements depend on the type of licence. For instance, the requirements to obtain a licence pursuant to Section 32(1) KWG for providing investment brokerage or investment advice are less tight than for guarantee or for safe custody business. In this regard, it makes a significant difference for regulatory purposes whether an institution is entitled to hold funds or assets for its clients because in this case the regulatory requirements are more comprehensive and stricter.

The newly introduced licence requirement for the crypto custody business under the KWG may be considered the first fintech-specific or at least fintech-focused licence requirement under German law. The corresponding changes to the KWG were made in the course of the implementation of the Fifth EU AML-Directive (Directive (EU) 2018/843) but without the legal necessity under EU law to make such changes of the KWG. The relevant Section 1(1a)(2) No. 6 KWG defines crypto custody business as custody, management and safeguarding of crypto values or private cryptographic keys used to hold, store or transfer crypto values as a service for others. Cryptographic values, which are (now explicitly) included in the catalogue of financial instruments under Section 1(11) sent. 1 No. 10 KWG, are defined as digital representations of value that are not issued or guaranteed by a central bank or a public authority, do not possess statutory status of currency or money, but are accepted by natural or legal persons as a means of exchange or payment, or which serve investment purposes and which can be transferred, stored and traded electronically. Consequently, the term crypto value includes not only crypto currencies like Bitcoin but also investment tokens. The broad definition of the terms crypto value and crypto custody business (including also the activities relating to private cryptographic keys) results in a wide scope of the new licence requirement. The KWG, however, provides for certain relief insofar as crypto custody service providers focusing on this type of financial service (i.e., that do not carry out any other regulated activities) do not have to meet all regulatory obligations applying to other providers of financial services. Instead, such crypto custody service providers are exempted from the general capital and liquidity requirements under the CRR (Regulation (EU) No. 575/2013) and some other rules. However, the requirements on the initial capital, reputation of the board members, proper business organisation and related reporting obligations do apply. The new licence regime for custody service providers also includes certain transitional provisions so that such service providers may adapt to the new requirements if they submit a complete application for the necessary licence until 30 November 2020. Further guidance with respect to crypto custody business and the transitional period has been provided by BaFin.12

Although it would exceed the given framework to elaborate on the licence requirements for every single fintech-relevant business model, it may be worth illustrating the licence requirement by reference to the robo-advice business models, as these have become popular in Germany in the recent years.

Generally speaking, a robo-adviser might be subject to a licence requirement pursuant to Section 32(1) KWG, in particular to provide investment brokerage, investment advice or portfolio management services. BaFin will only grant the necessary licence if, among other requirements, the applicant has at least €50,000 at its free disposal, if its managing directors are professionally qualified and with an impeccable reputation and if the applicant can prove that proper risk-management will be in place when the regulated business will be commenced.

By way of exception from this general licence requirement under the KWG, investment brokerage and investment advice may be provided under the less restrictive licence pursuant to Section 34f GewO; however, only specific financial products may be brokered or recommended under this privileged licence, which is granted not by BaFin but by the competent authorities in accordance with the laws of the relevant federal state. An additional exception is available for tied agents who closely cooperate with a licensed institution.

When robo-advisory models were introduced, some of the service providers offered robo-advice in the form of investment brokerage by connecting the supply of specific financial products to customers’ demand for financial instruments. These models try to implement a structure where the client stays in charge of the investment process so that the client makes the ultimate decision to buy or sell a financial instrument. There is, however, a thin line between investment brokerage and investment advice. Although BaFin did not pursue a strict approach until 2017, it then made clear that a robo-adviser provides investment advice if clients could get the impression that the investment proposals presented by the robo-adviser are tailored to their individual circumstances. The distinction between both types of investment services becomes relevant for the type of licence which is required and, in practice more important, with respect to the requirements which the robo-adviser must comply with in offering its services. Particularly the suitability report that an investment adviser must prepare and which is aimed to show how the recommended financial products suit the needs of the client is for many robo-advisers a bureaucratic obstacle they would like to avoid.

Both the stricter position of BaFin and the preference not to prepare for each investment a suitability report have led to many robo-advisers becoming licensed as portfolio managers. Providing such type of investment service, however, involves the obligation to adhere to a comprehensive set of rules of conduct so that robo-advisers must thoroughly analyse which route suits them best and which type of licence they need for their individual business model.

With respect to marketing regulations applicable to fintech companies in Germany, the general rule is that marketing must be fair, transparent and not misleading. These principles

---

13 More comprehensive capital and other requirements apply if the robo-adviser is entitled to hold the assets and funds of its clients.
15 Section 64(4) Securities Trading Act (WpHG).
16 Section 32(1) of the KWG within the meaning of Section 1 (1a)(2)(3) KWG.
follow from the Act against Unfair Competition (UWG) but are also included in some of the statutory provisions for financial services.\(^\text{17}\) Whether additional rules have to be taken into account depends primarily on the understanding of the term ‘marketing’.

As far as marketing for investment services within the meaning of Section 2(8) of the WpHG is concerned (including investment brokerage, investment advice, portfolio management, underwriting business etc.), it is rather difficult to distinguish marketing from the rules of conduct for service providers set out, inter alia, in Section 63 et seq. of the WpHG and a regulation promulgated thereunder (WpDVerOV) but also in various delegated regulations promulgated under MiFID II. These require that offerors of investment services provide their potential clients with mandatory information regarding, for instance, their products (e.g., key information sheets), potential conflicts of interest and inducements, and that they obtain certain information from their clients. Further, investment service providers must comply with detailed requirements set out in the Minimum Requirements for the Compliance Function and Additional Requirements governing Rules of Conduct, Organisation and Transparency (MaComp) which have been promulgated by BaFin.

Similar rules as for investment services apply to the marketing of funds under Section 298 et seq. of the KAGB. The information obligations for professional or semi-professional clients are less comprehensive than those for retail clients.

Regarding marketing for payment services, a comprehensive set of pre-contractual information obligations is provided for in the German Civil Code (BGB) in conjunction with Art. 248 of the Introductory Act to the BGB (EGBGB).

Further, marketing for certain fintech related services might entail the obligation to publish a prospectus. Such obligation is usually be triggered once a public offer for securities or financial assets has been made in accordance with the Prospectus Act (WpPG) or the Asset Investment Act (VermAnlG). In particular, the prospectus obligation under the VermAnlG may become relevant for fintech business models such as, for instance, crowdfunding or P2P lending platforms.

Fintech companies in Germany should therefore check whether marketing for their business might be captured by one of the comprehensive legal regimes for marketing.

\textbf{ii \hspace{1em} Cross-border issues}

As a general rule, the German regulations apply to each service provider conducting its business in Germany. This means that the rules – particularly the licensing requirement – not only apply if the service provider has its registered office in Germany, but also if it actively targets the German market cross-border.\(^\text{18}\)

Pure accessibility of the relevant services via the internet in Germany may be considered sufficient to assume that a service provider is actively targeting the German market. The regulations apply if the offeror of the relevant services intends the service to be used by

\(^{17}\) Section 63(6) WpHG, Section 302 KAGB and Section 23 KWG.

\(^{18}\) BaFin, Notes regarding the licensing for conducting cross-border banking business and/or providing cross-border financial services, April 2005, https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mgb_050401_grenzueberschreitend_en.html (24 March 2020).
German customers among users of different nationalities.\textsuperscript{19} If a service provider maintains its website in German, this is considered to be a strong indication of actively targeting the German market.

If, however, the provision of regulated services cross-border is concerned, the privilege to notify German regulators of existing licences from a home Member State within the European Economic Area (EEA) might offer an exception from this general rule, which may appear very strict at the first glance. The European ‘passport’ has been introduced for many regulated services such as, for instance, certain types of banking business, investment services as set out in Annex 1 of MiFID II and payment services. If a service provider has been licensed in its EEA-home Member State, the service provider may notify its competent supervisory authority of its intent to offer the regulated services also in Germany.\textsuperscript{20} Generally speaking, the service provider may commence the regulated business without a separate licence in Germany either on a cross-border basis or through a branch once the competent supervisory authority in the home Member State has informed BaFin, which subsequently has confirmed that the service provider may commence its business in Germany. In this scenario, the supervisory authority in the home Member State is generally responsible for the supervision of the service provider’s activities in Germany, subject to certain residual competences of BaFin and the German Federal Bank. The limitation of the European passport to institutions with registered seat in the EEA is one of the main reasons why the decision of the United Kingdom to leave the EU and the EEA (Brexit) has caused such a turmoil in the financial sector. If the EU and the United Kingdom do not endorse an agreement providing for a regulatory framework following the lapse of the transitional period under the Withdrawal Agreement, fintechs based in the United Kingdom providing regulated services will no longer have the opportunity to offer such services on a cross-border basis to customers in EEA Member States under the EU/EEA passport regime.

Another possibility for fintech companies to access the German market without being subject to a licence requirement is to cooperate with a licensed service provider, typically a bank. Such ventures are ‘white label structures’ where a regulated entity (fronting bank) effectively makes available its licence for the business activities of a third party. For this purpose the third party must subordinate its business to the bank’s management by granting instruction and control rights to the bank, which for regulatory purposes is responsible for the regulated services.

\section*{III DIGITAL IDENTITY AND ONBOARDING}

To date, there is no generally recognised digital identity available in Germany. However, it is possible to identify yourself electronically via the internet if the requirements of Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market are met. Details relating to this have been provided for in the Act on Trust Services (VDG).

\textsuperscript{19} Cf. Federal Administrative Court (Bundesverwaltungsgericht), decision of 22 April 2009, Az. 8 C 2/09, juris margin: 41.

\textsuperscript{20} BaFin, Freedom to provide services and freedom of establishment of credit institutions in the European Economic Area, https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Zulassung/EU-EWR-Kreditinstitute/eu-ewr-kreditinstitute_node_en.html (24 March 2020).
Regarding the onboarding process as required under the statutory anti-money laundering and counterterrorism rules, the Anti-Money Laundering Code (GwG), which was revised as part of the implementation of the Fifth EU AML Directive, includes various possibilities for remote identification. However, non-face-to-face business relationships or transactions may indicate higher AML risks\(^ {21} \) and thus may trigger enhanced customer due diligence requirements. In the past, BaFin published the standards for video identification, which are rather strict\(^ {22} \) and which were confirmed by BaFin in its guidance on the interpretation of the GwG published in December 2018\(^ {23} \). It remains to be seen whether and to what extent BaFin will adjust its administrative practice following the implementation of the Fifth EU AML Directive. However, given the recent legislative trends, an alleviation of the requirements is not to be expected.

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

Innovative funding solutions and business models related to payment services are typical areas in which fintech companies conduct business in Germany. Regulators have been struggling for some years to find a position on collective investment schemes balancing regulation to protect investors, in particular retail investors, and to allow innovative solutions that may also serve retail investors’ interests. Eventually German legislators concluded that the regulatory requirements applicable for already known investment business models shall generally (subject to limited privileges) also apply to collective investment schemes. Similarly, with regard to digital markets in general, German legislators and BaFin apply the technology-neutral principle of ‘same business, same risk, same regulation’. Therefore, the exact scope of the applicable requirements, in particular the assessment of whether a licence requirement under the KWG may be triggered, depends on the specific business model and should be reviewed on a case-by-case basis. The implementation of the Fifth EU AML Directive into German law has, at least to a certain extent, provided clarity on the regulatory qualification of activities in the cryptocurrency or cryptoassets business. As part of the implementation package, the German federal legislator introduced a legal definition of ‘crypto values’ and explicitly included these in the catalogue of financial instruments under the KWG.\(^ {24} \) In line with the Fifth EU AML Directive, the statutory definition of crypto values is broad in scope so that all potential uses of virtual currencies, including as a means of investment, are covered. On the international level, these various types of virtual units of value, described also as coins or tokens, are often referred to collectively as ‘cryptoassets’.\(^ {25} \) For more details, see Section V below.

---

21 See GwG, Annex 2 (factors for potentially higher risk).
24 See Section(11) No. 10 KWG.
i Peer-to-peer-lending

Whether and which regulatory rules apply for peer-to-peer-lending depends on the specific business model.

Crowdfunding based on donations the investors make to support a special project (crowd-sponsoring) is generally not subject to financial regulation. If, however, the investor benefits financially from his or her investment, for example by participating in future profits of the project (crowd investing) or by being reimbursed with or without interest (crowd-lending), special regulations apply. Such regulations may be distinguished as falling under supervisory law, consumer law and capital market law.

Supervisory law

Peer-to-peer lending in form of crowd investing or crowd-lending may entail consequences under German financial supervisory law for the lender, the borrower and the platform. The key concern relates to possible licensing requirements. In particular, the licensing requirement for lending business must be considered. A licence requirement is triggered if the lender acts commercially or in a manner that requires a commercially established business operation. It is sufficient if the lender intends to repeatedly engage in the lending business to make profits.

The taking of deposits commercially or on a scale that requires a commercially established business operation is also subject to a licensing requirement. These requirements may become relevant for all involved parties, for example the platform if it keeps the funds extended by the lenders until the funds are transferred to a single or several borrowers. If the platform performs such function and transfers funds from the investors to the borrowers, the platform may also be subject to a licensing requirement under the ZAG for providing payment services. The licensing requirement under the KWG may become relevant for the investors who provide the funds extended to a single or various borrowers too. Even the borrowers may be subject to a licensing requirement for conducting the deposit taking business when they receive the funds from the platform or the investors.

Given these regulatory restrictions, peer-to-peer-lending business models in Germany typically include a fronting bank that holds a licence for the lending and deposit-taking business. In these models, the fronting bank extends the loans to the borrowers, and the bank refinance the loans by selling the repayment claims arising under them to the platform for on-selling to investors or directly to investors who ultimately receive the repayment claim against the borrower. The various business transactions between the involved parties relating to the extension of a loan are interdependent by way of conditions precedent. Therefore, the bank is only obliged to extend the loan if investors have committed to provide sufficient funds for the purchase of the repayment claims arising under the loan. The platform, which is typically a fintech company, is acting in this model as a broker that brings together investors and borrowers.

28 Section 32(1) KWG in connection with Section 1(1) Sent. 2 No 2 KWG.
29 Section 32(1) KWG in connection with Section 1(1) Sent. 2 No 1 KWG.
Such structure is usually not critical for the investors as they only acquire a repayment claim, which is as such not subject to a licensing requirement, provided that the acquisitions do not occur under a framework agreement. In the latter case, a licensing requirement for providing factoring business could be triggered.\textsuperscript{30} For the borrowers this model is not problematic either. One might consider whether they engage in deposit-taking business. However, it is generally recognised under German law that it does not constitute deposit-taking to borrow funds from a licensed bank. The fronting bank has in this model the necessary licences so the remaining question is whether the platform performs business activities subject to a licence requirement. The platform might conduct the factoring business if it acquires the repayment claims from the bank prior to selling them on to investors. Usually, however, the factoring business can be avoided by certain structural arrangements. In this case the regulated activities of the platform consist of brokering loans (between the bank and the borrowers) and investments (between the platform or the bank and investors as purchasers of the repayment claims). These are activities which can be structured to avoid regulation under the KWG and to ensure that ‘only’ the licence requirements under Sections 34c and 34f GewO need to be met. BaFin considers the repayment claims brokered by the platform to be financial assets within the meaning of the VermAnlG and, therefore, financial instruments within the meaning of the KWG so that, in principle, the brokering activity could also be subject to a licensing requirement pursuant to Section 32(1) KWG which is, however, typically avoided by taking advantage of an exception.

\textbf{Consumer law}

In Germany, as in the European Union generally, relatively strict consumer protection rules apply. This is also the case for consumer loans. Consequently, a direct contract between the lender and the borrower brokered by a peer-to-peer lending platform triggers far-reaching information obligations for the lender under Section 491 et seq. BGB, provided that the lender acts commercially and the borrower is a consumer. Given the typical structure for peer-to-peer lending platforms in Germany, the fronting bank implemented in the structure must typically comply with these obligations.

Further, given that peer-to-peer lending platforms typically offer their services online, the consumer protection rules on distance selling must be considered (Section 312a et seq. BGB). These rules are based on EU law and should in general not differ in the EU Member States.

\textbf{Capital market law}

Generally speaking, the WpPG and the VermAnlG has to be considered if the regulatory framework for crowdfunding and crowd-lending platforms is analysed under German law from a capital market point of view.

The VermAnlG generally applies to profit participating loans, subordinated loans and all other investments that grant a claim to interest and repayment. If such investments are publicly offered, a prospectus or at least an information sheet concerning the investment must be published, unless certain exceptions apply. One of these is explicitly directed to internet platforms engaging in crowd-investment (Section 2a VermAnlG). Under this

\textsuperscript{30} Section 1(1a) Sent. 2 No 9 KWG.
exception, the obligation to publish a prospectus does not apply to investments that are only brokered via the internet and do not exceed low thresholds ranging from €1,000 to €10,000 per investment. Even if this exception applies, an information sheet must be published.

Should a crowdfunding platform issue or publicly offer securities within the meaning of the WpPG, a prospectus must, subject to certain limited exceptions, also be published. The WpPG obligations, however, have not yet gained material significance in the German fintech market, except for the very few fintech companies using securitisation to refinance. This might change in the future owing to the rise of ICOs.  

ii  Payment services

The payment services sector was one of the first in the German financial industry where fintech companies became active and visible. This is one of the reasons for fragmentation of the payment services market, which has recently begun to consolidate. Nevertheless, the revised Payment Services Directive (EU) 2015/2366 (PSD II), which has been implemented into German law with effect from 13 January 2018, offers new business opportunities especially for nimble fintech companies. The reason for this is that account information services and payment initiation services as new payment services were introduced under the revised ZAG. The providers of such services now have a legal claim for access to payment accounts against the banks that maintain such payment accounts for their customers. This is perceived as a potential game changer because the traditional banks can no longer prevent their competitors from accessing the accounts of customers who consent to such access (open banking). However, experiences so far suggest that it will take some time before the necessary APIs work as required. Some market observers have already criticised credit institutions for using the PSD II rules as an instrument to prevent competition by fintechs, e.g., by no longer offering the previously established connections via FinTS.

Further, new business opportunities come with additional regulatory burdens. Providing payment services is generally subject to a licence requirement, unless certain exceptions apply. The scope of this licence requirement has been expanded to comprise the providers of account information and payment initiation services even though these service providers do not acquire at any time possession of their customers’ funds. On account of this consideration, the regulatory requirements for a licence to provide payment initiation or account information services are less strict than for a licence to provide traditional payment services.

Recent amendments of the ZAG aim to foster technological innovation and competition on the payment market. 32 Under the relevant provisions (Section 58a ZAG) – which has been labelled by some market observers as ‘Lex Apple Pay’ – payment services providers and e-money issuers have the right to obtain access to certain key technical infrastructure. ‘System companies’ contributing through technical infrastructure services to the provision of payment services or the conduct of e-money business in Germany are obliged, upon request of a payment services provider or e-money issuer, to make such technical infrastructure services available and provide necessary access against consideration and without undue delay. The obligation does not apply if the relevant technical infrastructure is used by no more than 10

31 See in more detail at Section V.ii.
payment services providers or e-money issuers or if the company has no more than 2 million registered users. The company may also deny access in case of objective reasons, for example, if the security and integrity of the technical infrastructure services would be jeopardised. The new statutory rules are not based on EU law and are considered to be the reaction to some system providers refusing to open their systems to facilitate more competition in the area of mobile payments.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

i Cryptocurrencies

Cryptocurrencies such as Bitcoin undoubtedly constitute a challenge for the German law from regulatory, civil law and tax perspectives. A certain level of conceptual clarity has been achieved by the legal definition of crypto values (such as Bitcoin) in connection with the implementation of the Fifth EU AML Directive into German law. Crypto values are now included in the catalogue of financial instruments under the KWG so that various activities relating to crypto values are clearly within the scope of certain licence requirements. Further, the crypto custody business has been introduced as a new type of financial service, which is subject to a licence requirement under the KWG.

Crypto values are defined as digital representations of a value that is not issued or guaranteed by a central bank or a public authority, does not possess a statutory status of currency or money, but which is accepted by natural or legal persons as a means of exchange or payment, or which serves investment purposes and which can be transferred, stored and traded electronically. This broad definition is aimed at comprising any uses of virtual currencies, including as a means of investment. So far the definition of crypto values includes not only tokens with exchange and payment functions (including cryptocurrencies), which may anyway fall under the scope of financial instruments as the ‘units of account’ within the meaning of Section 1(11) sent.1 No. 7 KWG, but also tokens used for investment. Such security or investment tokens may also qualify as investment products, debt instruments or units in collective investment schemes under Section 1 (11) sent. 1 Nos. 2, 3 or 5 KWG.33

Not covered by the definition of crypto values are domestic and foreign legal tender, electronic money, monetary value stored on payment instruments falling under the limited network exemption within the meaning of PSD II and payment transactions of providers of electronic communications networks or services.34 Also not covered are electronic vouchers for the purchase of goods or services from the issuer or a third party that are intended to have an economic function in relation to the issuer only through redemption and that are therefore not tradable and, due to their design, do not reflect investor-like expectations regarding the performance of the voucher or the general business performance of the issuer or a third party in terms of value or accounting.35

34 See Section 2(1) Sent. 2 No. 10 and 11 ZAG.
The amendments with respect to crypto values reflect to a certain extent the previous administrative practice of BaFin that took the first steps towards the regulation of cryptocurrencies in Germany by adopting a broad interpretation of the term 'financial instrument' within the meaning of the KWG. This approach was partially criticised and not shared in a ruling of a higher regional court in criminal proceedings.36

The recent changes of the KWG has resolved the controversy on the qualification of cryptocurrencies as financial instruments and has insofar contributed to more legal clarity. It should be noted, however, that the German legislator only changed the definition of 'financial instrument' for the purpose of the licensing requirement but not with regard to the conduct rules set out in the WpHG, which effectively reflect the MiFID II provisions. Therefore, a service provider operating a market place for cryptocurrencies may fall within the licence requirement for an operator of multilateral trading facilities within the meaning of the KWG but may not be obliged to adhere to the rules of conduct set out for such operators in the WpHG.

Against this background, one should thoroughly analyse the legal risks related to relevant business models and assess whether and which licence requirements and conduct rules may apply. In particular, buying and purchasing cryptocurrencies in the service provider’s own name for the account of others may constitute banking business in the form of principal brokering business.37 Further, brokering cryptocurrencies may constitute for licensing purposes investment brokerage,38 whereas advising on the purchase or sale of cryptocurrencies may be considered investment advice.39 Also the operation of a platform on which cryptocurrencies can be traded may qualify as a multilateral trading platform within the meaning of Section 1(1a) sent.2 No. (1b) KWG and may, therefore, be subject to a licence requirement.40 The activity involving custody, management and safeguarding of crypto values or private cryptographic keys may also fall within the scope of the newly regulated crypto custody business. This new type of financial service and the related licence requirement may be relevant for domestic companies as well as cross-border service providers and their agents that intend to or have already been offering such services.41

However, neither the mining, nor the purchase or sale of cryptocurrencies in one’s own name and for one’s own account is subject to a licence requirement. Therefore, cryptocurrencies may generally be used as means of payment and generated by mining without any special permission.

From a civil law perspective, many questions have not yet definitively been answered. The uncertainty starts with the applicable jurisdiction and laws generally for a cryptocurrency. These questions become relevant if, for instance, cryptocurrency units are transferred or pledged. Further, it is still unclear which disclosure and information obligations apply in cryptocurrency transactions.

36 Higher Regional Court of Berlin (Kammergericht Berlin), decision of 25 September 2018 – (4) 161 SS. 28/18 (35/18).
37 Section 1(1) sent. 2 No. 4 KWG.
38 Section 1(1a) sent. 2 No. 1 KWG.
39 Section 1(1a) sent. 2 No. 1a KWG.
41 See Section II above.
Interestingly, the usually complex tax analysis has at least partly been clarified for cryptocurrencies through a decision by the European Court of Justice (CJEU).\textsuperscript{42}

According to the principles of this decision that were incorporated into German tax law,\textsuperscript{43} exchanging regular currencies into Bitcoin (or comparable cryptocurrencies) and vice versa shall be tax-free with respect to value added tax according to Section 4 No. 8b of the Turnover Tax Code (UStG). In addition, using Bitcoin or comparable cryptocurrencies as payment and the process of mining are tax-free.

Other transactions concerning cryptocurrencies may, however, be affected by tax law.

From an accounting perspective, cryptocurrency units like Bitcoin are transferable so that it appears necessary to account for them as assets on the balance sheet.

If they qualify as assets that support the business for only a short period (current assets), they may have to be recorded as ‘other assets’ according to Section 266 (2) B II No. 4 of the Commercial Code (HGB).\textsuperscript{44} If the cryptocurrency units qualify as assets that support the business for a long period (fixed assets) they should be taken accounted for as acquired immaterial assets according to Section 266(2) A I No. 2 of the HGB.\textsuperscript{45}

\textbf{ii Initial coin offerings}

Initial coin offerings (ICOs) are sales of virtual tokens to raise funds for general corporate purposes or a specific project typically described in more detail in a White Paper. Depending on the structure of the ICO, tokens may be bought with regular or virtual currencies and may grant specific rights such as participation rights and profit shares, or no right at all. While the discussions and structures of ICOs and tokens are still in flux, tokens that can be offered in an ICO may be categorised as follows:

\begin{itemize}
  \item[a] Cryptocurrency tokens are meant to pay for goods or services external to the platform or not only exclusively between the platform and its users but also between users.
  \item[b] Utility tokens are supposed to convey some functional utility to token holders other than or in addition to payment for goods or services, in the form of access to a product or service. These tokens come with particular rights, such as a right of access to a future service, a right to redeem the token for another token or service or voting rights which often are designed to shape the functionality of the product.
  \item[c] Security tokens are comparable to traditional securities set out in Article 4(1)(44) MiFID II such as conventional debt or equity instruments.\textsuperscript{46}
\end{itemize}

This rough categorisation – which corresponds to the general approach pursued by BaFin – illustrates that tokens may differ significantly. Following the amendments to the KWG, as from 1 January 2020, tokens with exchange and payment functions and tokens used for investment, for example, security tokens and investment tokens, are likely to fall within the

\textsuperscript{42} Cf. European Court of Justice, decision of 22 October 2015, C-264/14, V, Hedqvist.
\textsuperscript{44} Kirsch / von Wieding, Bilanzierung von Bitcoin nach HGB, BB 2017, 2731, 2734.
\textsuperscript{45} Kirsch / von Wieding, Bilanzierung von Bitcoin nach HGB, BB 2017, 2731, 2734.
\textsuperscript{46} Blockchain Bundesverband, Finance Working Group, Statement on token regulation with a focus on token sales (undated), p. 3.
broad definition of cryptographic values and thus constitute financial instruments under KWG (aside from possible classification of such tokens as other types of financial instruments, which is to be assessed on a case-by-case basis).47

Consequently, each ICO must be thoroughly analysed with respect to its regulatory and capital market requirements. BaFin determines the applicability of the relevant legislation including the KWG, the ZAG, the WpPG, the KAGB and the VermAnlG case by case, depending on the specific contractual arrangements. Where tokens resemble participation rights that might be classified as securities under the WpPG or capital investments under the VermAnlG, a prospectus for the marketing of the tokens may be required. One might question, however, whether a fully digitised token constitutes a security within the meaning of the WpPG, as under German securities law such a security requires a certificate. In light of this general concept, the first BaFin-approval of a prospectus for a public offer of fully digitalised blockchain-based tokens under the WpPG regime, in February 2019, was quite unexpected. Given the current legal framework for securities, it is not entirely clear yet whether this route involves various legal risks despite the approval by BaFin. It seems that clarity in this regard requires an amendment of the German securities laws explicitly permitting fully digitalised offerings of securities. The necessary changes of the relevant laws are already being discussed. The German federal government demonstrated its intention to support such changes when the German Federal Ministry of Finance and the German Federal Ministry of Justice and Consumer Protection published a joint paper concerning the future regulatory framework for blockchain-based securities and crypto-tokens, aimed to foster innovation and investor protection.48

In addition to a prospectus requirement, any professional service provided in connection with the trading of tokens – including an agreement to acquire, or the sale or purchase of tokens – when qualified as units of account or crypto values – would, as a general rule, require a licence from BaFin.49

Even if an obligation to publish a prospectus does not exist, issuers of tokens should be aware that consumer protection laws might apply to the sale of tokens via internet. So, the underlying contract may qualify as a distance contract resulting in information obligations according to Section 312(i) of the BGB. Provided that the contract is considered as financial service, further information must be provided according to Section 312(d) of the BGB.50

iii Money laundering rules

Tokens and cryptocurrencies in general are perceived as highly susceptible to money laundering and terrorism financing. In this respect, a certain level of clarity with regard to the applicability of the AML regime has been provided by the law implementing the Fifth EU-AML Directive in Germany, in force since 1 January 2020. As already outlined above, the law introduced a

49 See in more detail in Section V.i.
broad definition of crypto values and classified them as financial instruments under the KWG. In principle, the scope of the definition generally includes tokens with exchange and payment functions (e.g., cryptocurrencies) and tokens used for investment (e.g., security tokens and investment tokens).\textsuperscript{51} This generally means that services concerning cryptocurrencies and tokens, for instance, buying and purchasing cryptocurrencies in the service provider’s own name for the account of others, advising on the purchase or sale of cryptocurrencies or operation of a platform on which cryptocurrencies can be traded may fall under the scope of regulated services and require a KWG licence for, in particular, principal brokering business,\textsuperscript{52} investment brokerage,\textsuperscript{53} investment advice\textsuperscript{54} or operation of a multilateral trading platform.\textsuperscript{55} In addition, the management and safeguarding of crypto values or private cryptographic keys may require obtaining a KWG licence if other general statutory prerequisites under KWG (in essence, commercial character or a scale that requires a commercially organised business undertaking) are fulfilled. Services providers whose activities fall within the scope of the KWG-licence requirements are obliged entities within the meaning of the GwG and must, therefore, adhere to the duties set out therein. These include the obligation to conduct adequate customer due diligence, to implement adequate risk management systems aimed at preventing money laundering and terrorism financing and, as appropriate, notifying the Financial Intelligence Unit of any suspect transactions as well as fulfilling respective reporting obligations in relation transparency register. Nonetheless, even prior to the implementation of the Fifth EU-AML Directive into German law cryptocurrency and ICO service providers were often required to obtain a KWG licence and, as a result, comply with the German AML requirements. This was owing to the broad interpretation of the term ‘financial instrument’ within the meaning of the KWG according to BaFin’s previous administrative practice.\textsuperscript{56}

Further, an interesting and not fully clarified question is whether the issuer of tokens in an ICO may be subject to such obligations under the GwG. This may well be the case because such an issuer might be regarded as a person trading in goods within the meaning of Section 1 (9) GwG.\textsuperscript{57} For persons trading in goods, however, the full set of obligations under the GwG does not apply; instead, they need only – in the absence of a specific suspicion – identify their counterparty if they pay or receive a cash payment of at least €10,000 (Section 10(6) GwG).

VI OTHER NEW BUSINESS MODELS

Generally speaking, it seems difficult to identify totally new business models in the past one or two years. Instead, one can observe enhanced efforts to find specific uses for blockchain technology and for artificial intelligence.

\textsuperscript{52} Section 1(1)(2)(4) KWG.
\textsuperscript{53} Section 1(1a)(2)(1) KWG.
\textsuperscript{54} Section 1(1a)(2)(1a) KWG.
\textsuperscript{55} Section 1(1a) Sent.2 No. (1b) KWG.
\textsuperscript{56} See Section V above.
These efforts can be illustrated by the cooperation of Deutsche Bundesbank with Deutsche Börse aimed to develop solutions for a securities settlement system which facilitates the delivery of securities against virtual currency units on the basis of the distributed ledger technology.58

Participants in the capital markets in general appear to seek increasingly successful business models exploiting the potential of fintech. The first placings of promissory notes and commercial papers (even though these papers have not been governed by German law) have been made in Germany by taking advantage of the blockchain technology and of highly digitalised platforms.

Further, how artificial intelligence could support anti-money laundering compliance and the compliance function in general, which is sometimes called ‘digital compliance’, is also being investigated. In this regard, however, it seems too early to maintain that new business models have already established themselves on the German market.

In general, the operation of business models involving the use of AI is subject to the regulatory requirements applicable to already known business models in line with the technology-neutral approach of ‘same business, same risk, same regulation’. This means that for each relevant fintech business model, careful analysis should judge whether it falls within the scope of one or several regulated services and which regulatory requirements apply. In essence, the KWG-licensed institutions using programs and algorithms involving AI must ensure that they maintain a proper business organisation,59 in particular an adequate and effective risk management, and that the use of such programs and algorithms is in line with such general regulatory requirements. This includes processes for determining and safeguarding the sustainability of services, internal control procedures and internal control systems, adequate contingency plans, especially for IT systems, complete documentation of business operations permitting seamless monitoring by BaFin as well as compliance with outsourcing requirements. The exact arrangement of the business organisation should be appropriate for the nature, scope, complexity and risk content of the institution’s business activities. In this regard, the minimum requirements for risk management in BaFin’s Circular No. 09/2017 (MaRisk)60 and with the supervisory requirements for IT in BaFin’s Circular No. 10/2017 (BAIT) have to be met.61

With respect to the use of algorithms by KWG-licensed institutions BaFin has recently confirmed its approach that it does not grant general a priori approvals for the use of algorithms in decision-making processes and that its administrative practice is technology-neutral.62 The legal reasoning behind this approach is generally twofold: the nature of the risk-oriented and

59 See Section 25a KWG.
ad hoc financial supervision on the one hand and the lack of a statutory basis for general a
priori algorithms approvals on the other.\textsuperscript{63} As to the former, the supervisory requirements do
not primarily concern the algorithm itself; instead, the focus of supervision is on the entire
decision-making process in which the relevant algorithm is embedded – therefore compliance
with general requirements on proper business organisation and risk management plays a
key role.\textsuperscript{64} With respect to the lack of a statutory legal basis for algorithms approval two
exceptions should be noted in which the regulation of the use of algorithms may be derived
from the law itself (e.g., determination of capital and solvency requirements). However, even
in such cases the supervisory authorities will not grant an a priori approval. Instead, they
conduct a risk-oriented assessment of the relevant decision-making and other procedures
taking into account the available data and its quality.\textsuperscript{65}

The approach of technological neutrality applies generally also to the regulation of
KWG licence requirements. In this respect, one might consider high-frequency trading (a
special form of proprietary trading)\textsuperscript{66} as an exception. Per definition, high frequency trading
includes the use of algorithms for the sale and purchase of financial instruments.\textsuperscript{67} While
German supervisory rules generally do not provide for specific notification obligations in the
case of the use of particular software or algorithms, high frequency trades have to adhere to
specific notification requirements.\textsuperscript{68}

Worth mentioning in the context of recent and successful fintech-related business
models is the increasing digitalisation in the insurance sector. New service providers have
evolved that primarily broker insurance via smart phones quickly and simply. Certainly, such
brokers must also comply with the general information duties relating to the brokerage of
insurance contracts.

Also successful, but not strictly new, are product comparison websites, which have
become very popular with price-conscious consumers. The influence of such offerings on the
market is governed by the general competition rules. These include that price comparison
tests must be performed in a competent manner, seek to be objectively accurate and be neutral.\textsuperscript{69} Finally, the incorporation of so-called fintech banks is noteworthy in connection
with new business models. These fintech banks hold a comprehensive licence to conduct
banking business but still perceive themselves to be fintech companies. Their business model
is based on digitalisation, and they partly offer white-label solutions, namely they may
seek to cooperate with other fintech companies that need licensed banks for their business

\textsuperscript{63} See BaFin, Generelle Billigung von Algorithmen durch die Aufsicht? Nein, aber es gibt Ausnahmen,
Algorithmen.html (25 March 2020) (available only in German).

\textsuperscript{64} Cf. BaFin, Generelle Billigung von Algorithmen durch die Aufsicht? Nein, aber es gibt Ausnahmen,
Algorithmen.html (25 March 2020) (available only in German).

\textsuperscript{65} Cf. BaFin, Generelle Billigung von Algorithmen durch die Aufsicht? Nein, aber es gibt Ausnahmen,
Algorithmen.html (25 March 2020) (available only in German).

\textsuperscript{66} Cf. Section 1(1a) sent. 2 (4d) KWG.

\textsuperscript{67} Cf. BaFin, Generelle Billigung von Algorithmen durch die Aufsicht? Nein, aber es gibt Ausnahmen,
bj_2003_Algorithmen.html (25 March 2020) (available only in German).

\textsuperscript{68} Cf. Section 80(2) sent.5 WpHG

\textsuperscript{69} BGH, decision of 9 December.1975 - VI ZR 157/73, ‘Warentest II’.

© 2020 Law Business Research Ltd
model. This illustrates that some fintech banks position themselves as ‘platform banks’, where cooperation partners may find specific service offerings that they can use to complement their own products or services.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

i Intellectual property

A business model as such cannot be protected by copyright law. Therefore, it is not uncommon for successful fintech business models to be copied and optimised. Computer programs, however, that are characterised by a minimum of individuality and originality are subject to copyright protection according to Section 2 of the Act on Copyright and Neighbouring Rights (UrhG).

Under German law copyright can be neither registered nor transferred, since the copyright itself emerges the moment the piece of work, such as the software, is created by its actual originator. The capacity of being the originator is strictly connected to a natural person and may therefore not be transferred. Obviously the lack of registration leads to various practical problems that often result in lawsuits. Nonetheless, a licence may be granted enabling the holder to make use of the piece of work in every or in particular matters (Section 31 of the UrhG). Employees and their employers implicitly agree on a full licence by drafting the employment contract. Therefore, the employer is allowed to make use of the piece of work. Concerning computer programs, another rule applies (Section 69b of the UrhG), granting the employer even more rights. Unless agreed otherwise, the employee is owed no compensation.

ii Data protection

Generally speaking, data protection is governed the General Data Protection Regulation (GDPR), which replaced to a material extent the previous version of the Federal Act on Data Protection as of 25 May 2018 without, however, changing the fundamental principles of German data protection law. The GDPR intends to prevent the collection and use of data related to individuals unless it is duly necessary to do so (Article 1 of the GDPR). Data are considered to be related to individuals if the responsible body has the legal means that enable it to identify the data subject.

Collection and processing of data related to individuals is only permitted if it is explicitly allowed by law or if the data subject consents (Article 6(1) GDPR). Additionally, the user must be informed about nature, extent and purpose of data collection.

Digital profiling has to comply with the general principles stated above. The GDPR does not regulate digital profiling as such but focuses on some of its typical forms: firstly, the automated individual decision-making, including profiling, must comply with Article 22 of the GDPR; secondly, a decision that produces legal effects on the data subject or has a similarly significant influence on the data subject must not be based solely on automated

71 Cf. Bullinger, Wandtke/Bullinger, Praxiskommentar zum Urheberrecht, edition 4, Section 7 rec. 3.
72 Cf. Benkard, Patentgesetz, edition 11, Section 15 rec. 5.
73 Cf. Wandtke, Wandtke/Bullinger, Praxiskommentar zum Urheberrecht edition 4, Section 43 rec. 50.
75 CJEU, decision of 19 October 2016 – C-582/14.
processing (Article 22(1) GDPR). However, Article 22(1) GDPR shall not apply, if the decision: (1) is necessary for entering into, or performance of, a contract between the data subject and the data controller; (2) is authorised by law to which the controller is subject and that also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or (3) is based on the data subject’s explicit consent (Article 22(2) GDPR).

VIII YEAR IN REVIEW

Considering the developments in the fintech sector within the past 12 to 18 months, the following trends appear worth emphasising.

Overall, it seems that the fintech market in Germany has continued to demonstrate growing maturity and has recently reached a consolidation phase. This, and the fact that business models of German fintech companies have been able to implement commercially viable business models, is illustrated by one of the German fintech banks that became the first German fintech ‘unicorn’, with a market evaluation of more than €1 billion by significant financings in 2018. However, scaling their operations is still difficult for many local fintechs, which may also be a result of the increasing efforts of incumbent institutions to take advantage of the lessons learned from fintechs concerning innovation and customer experience. Traditional players in the financial sector use these insights not only by establishing cooperations and partnerships with fintech companies and including fintechs in their value chains but also by developing their own digital offerings.

ICOs and cryptocurrencies continue to be among the dominant topics in the fintech sector. This can be illustrated by the implementation of the Fifth EU-AML Directive into German law. The broad legal definition of crypto values introduced by the German legislator not only results in enhanced AML obligations for service providers engaging in the cryptocurrency business but also introduces a licence requirement for the crypto custody business.

The application of distributed ledger technology for other use cases remains a challenge, but market participants have deployed significant efforts to identify and realise corresponding business models, for instance, in the field of capital markets or supply chain finance.

The relevance of distributed ledger technology has also been recognised by politicians and by supervisory authorities. It seems that specific regulation of blockchain-based business models will be introduced rather sooner than later. The German legislator expressed its intention not to wait for a harmonised solution at the EU-level, but to initiate a blockchain initiative also involving specific legislation aimed at fostering business models using the distributed ledger technology.

Further, the introduction of the new Section 58a ZAG suggests that the implementation of PSD II may not be considered the final step towards increased competition and innovation in the payment sector. It appears, however, that technical constraints (the removal of which does not seem to be the primary objective of incumbent players) have prevented account information and payment initiation providers to take full advantage of the business opportunities expected as a consequence of PSD II.
IX  OUTLOOK AND CONCLUSIONS

Given the numerous initiatives at an international, EU and national level dealing with the regulatory challenges of fintech, further specific regulation has to be expected. A recent illustration of this trend was the implementation of the Fifth EU-AML Directive into German law. This, however, does not need to be detrimental to fintechs and their offerings. Instead, this is a chance for a reliable legal framework to foster trust and create an attractive climate for investors. Further, German politicians have recognised that the legislation needs to provide a legal environment that promotes innovative solutions. Whether this will lead to the introduction of an option for EU Member States to elect a ‘sandbox model’ remains to be seen. The regulatory authorities in Germany would still not welcome such an option. Instead, it is currently more likely that special legislation will be introduced in Germany that addresses the needs of blockchain-based business models. Further, there are some indications (e.g., the harsh sanctions regime) that the GDPR might turn out to be an obstacle for future prosperity of the fintech sector. In particular, it is questionable how the requirements under the GDPR and, in particular, the ‘right to be forgotten’ can be fully implemented by the blockchain-based services and products. Finally, new developments can be expected in the area of big data and AI.
As a jurisdiction, Guernsey’s economy is built largely around the provision of financial services to a global marketplace. As such, fintech businesses operate within the broader regulatory regimes established to maintain Guernsey’s financial services status internationally. Fintech is expected to play an ever increasing role in Guernsey’s financial services sector, and significant attention and resourcing is being devoted to creating a regulatory environment wherein the latest technological developments can be utilised while maintaining the controls necessary to ensure continuity of Guernsey’s reputation. As a result of this, Guernsey is increasingly fintech friendly. Fintech is one of the core focuses for the island’s ongoing development, a position underscored by its inclusion as one of the pillars of the island’s strategic development framework as set out in the States of Guernsey and Guernsey Finance’s ‘Financial Services Policy Framework’.

The Guernsey Financial Services Commission (GFSC) is primarily responsible for financial services regulation on the island. It has introduced its Innovation SoundBox to serve as a GFSC hub for enquiries regarding innovative financial products and services.

The Innovation Soundbox is intended to assist prospective innovative or start-up financial services businesses with access to regulators and GFSC policymakers, transparency on the Bailiwick of Guernsey’s regulatory requirements and guidance on the regulator’s approach to innovative propositions. While the Innovation Soundbox is not restricted to fintech issues, it has been broadly interpreted as a response to the potentially disruptive effects of fintech upon financial services business and regulation more generally. Similarly, the GFSC has been working internationally to develop common regulatory approaches to innovative propositions as part of the Global Financial Innovation Network (GFIN).

In terms of local development of fintech, while this has been led by the private sector, Guernsey has established the Digital Greenhouse to act as a focal point for the growth of the digital and creative sector locally, offering a dedicated space to accelerate start-up and growth activity in Guernsey.

---

1 Wayne Atkinson is a group partner at Collas Crill LLP.
II REGULATION

i Licensing and marketing
To date, Guernsey has chosen not to create fintech-specific regulation or legislation. Fintech companies are therefore subject to regulation only within the wider Guernsey financial services regulatory regimes applied by the GFSC to the extent these regimes apply. The GFSC has indicated that they will treat applications related to Fintech in the same manner and apply the same standards of control as they would in respect of more traditional applications.

The most applicable of these laws is the Protection of Investors (Bailiwick of Guernsey) Law 1987, as amended (the POI Law), which sets out nine ‘restricted activities’ that cannot be carried out, by way of business by a Bailiwick body, in relation to a ‘controlled investment’ (as defined in the POI Law), without licensing. These are promotion, subscription, registration, dealing, management, administration, advising, custody and operating an investment exchange. Failure to have the appropriate licence when carrying on controlled investment business is a criminal offence.

The definition of controlled investment is a broad one, including investments in collective investment schemes, general securities and derivatives (these terms are themselves defined within the POI Law), meaning the licensing regime of the POI Law has the capacity to capture a number of fintech business models and related activities. The positioning of cryptocurrencies, coins and tokens within or outside this definition will likely be determined on a case-by-case analysis of the specific rights and assets attributable to a coin, token or cryptocurrency.

The marketing of a fintech product in Guernsey would therefore be regulated under the POI Law to the extent that such a product constituted a controlled investment in line with the above definition.

Additionally, the POI Law puts in place a regime for the regulation of investment funds domiciled in Guernsey. Businesses that require licensing under the POI Law are required to have in place client identification and broader anti-money laundering processes as well as meeting various other standards designed to protect investors. For licensees, the GFSC will focus upon adequacy of resourcing, controls and the provision of suitably skilled personnel, whereas for funds, among other things, controls around valuation, liquidity, custody and the protection of assets are key.

In addition to the POI Law, the Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law 2008 (the NRFSB Law) creates a public register of non-regulated financial services businesses (and as such does not apply to licensed financial services businesses). The NRFSB Law is part of the Bailiwick’s framework for anti-money laundering (AML) and combating the financing of terrorism (CFT). The framework, including the registration, has no effect on the operational requirements and activities of a registered business except for the carrying out of AML/CFT measures.

The NRFSB Law applies to a number of types of financial services businesses, some of which have direct or indirect applicability in the fintech space, including:

a lending;
b financial leasing;

3 Schedule 1, Protection of Investors (Bailiwick of Guernsey) Law 1987.
4 Schedule 1, NRFSB Law.
operating a money service business (including, without limitation, a business providing money or value transmission services, currency exchange (bureau de change) and cheque cashing);

facilitating or transmitting money or value through an informal money or value transfer system or network;

issuing, redeeming, managing or administering means of payment. Means of payment includes, without limitation, credit, charge and debit cards, cheques, travellers’ cheques, money orders and bankers’ drafts and electronic money;

providing financial guarantees or commitments;

trading (by way of spot, forward, swaps, futures, options, etc.) in money market instruments (including, without limitation, cheques, bills and certificates of deposit), foreign exchange, exchange, interest rate or index instruments, and commodity futures, transferable securities or other negotiable instruments or financial assets;

participating in securities issues and the provision of financial services related to such issues;

providing settlement or clearing services for financial assets including, without limitation, securities, derivative products or other negotiable instruments;

providing advice to undertakings on capital structure, industrial strategy or related questions, on mergers or the purchase of undertakings except where the advice is provided in the course of carrying on the business of a lawyer or accountant;

money broking;

money changing;

providing individual or collective portfolio management services or advice;

providing safe custody services;

providing services for the safekeeping or administration of cash or liquid securities on behalf of clients;

carrying on the business of a credit union;

accepting repayable funds other than deposits; and

otherwise investing, administering or managing funds or money on behalf of other persons.

Businesses carrying on the operations listed above on an incidental or occasional basis may not be required to register with the GFSC or to meet the AML/CFT regulations and rules in the GFSC’s Handbook for Financial Services Businesses On Countering Financial Crime and Terrorist Financing.

The test for exclusion from the requirements of the NRFSB Law requires businesses to meet all of the criteria below:

- the total turnover of that business, plus that of any other financial services business carried on by the same person, does not exceed £50,000 per annum;
- no occasional transactions are carried out in the course of such business; that is to say, any transaction involving more than £10,000, where no business relationship has been proposed or established, including such transactions carried out in a single operation or two or more operations that appear to be linked;
- the turnover of such business does not exceed 5 per cent of the total turnover of the person carrying on such business;

---

5 Section 3, the NRFSB Law.
the business is ancillary, and directly related, to the main activity of the person carrying on the business;

in the course of such business, money or value is not transmitted or such transmission is not facilitated by any means;

the main activity of the person carrying on the business is not that of a financial services business;

the business is provided only to customers of the main activity of the person carrying on the business and is not offered to the public; and

the business is not carried on by a person who also carries on a licensed financial services business.

ii Cross-border issues

Guernsey is a leading centre in the global funds industry, which in recent years has included a focus on technology funds. Guernsey has never been a Member State of the European Union, but has put in place all of the infrastructure needed to allow funds and other similar investment structures launched in Guernsey to be marketed to both UK and EU investors. Guernsey has implemented a voluntary regime that mirrors the requirements of the Alternative Investment Fund Managers Directive (AIFMD). While the full AIFMD passport has not yet been extended to non-EU ‘third countries’, Guernsey funds are able to market to EU investors through the National Private Placement Regimes of EU Member States.

The GFSC is one of 12 financial regulators or related organisations that have collaborated on the establishment of the GFIN, building on a proposal in early 2018 to create a ‘global sandbox’. This project will seek to provide a more efficient way for innovative firms to interact with regulators, helping them navigate between countries as they look to scale new ideas. It will also create a new framework for cooperation between financial services regulators on innovation-related topics, sharing different experiences and approaches.

Among the primary functions of the GFIN is to allow collaboration and share regulatory experience of innovation in respective markets, including emerging technologies and business models among which issues highlighted were artificial intelligence, distributed ledger technology, data protection, regulation of securities and initial coin offerings (ICOs), know-your-customer and anti-money laundering.

III DIGITAL IDENTITY AND ONBOARDING

A barrier to the electronic onboarding of clients in the financial services industry has traditionally been the need for certified copies of client due diligence information in order to permit the completion of necessary anti-money laundering processes. The latest version of the GFSC’s Handbook for Financial Services Businesses On Countering Financial Crime and Terrorist Financing explicitly addresses electronic methodologies for onboarding clients and obtaining the necessary certifications digitally (e.g., by way of an app that takes control of a smartphone’s camera to photograph potential clients holding their identification documents) for later verification.

While responsibility for anti-money laundering procedures always remains with the board of the licensed financial services business in question, a number of service providers have begun operating a client identification service that financial services businesses can contract with allowing clients to identify themselves once to the client identification service and then allow this data to be shared digitally with other businesses as necessary. Notable among these
is the ID Register, which at the time of writing has an authenticated due diligence record of more than 25,000 investors shared among 274 (largely investment fund) clients and around 750 pension plans.

Guernsey does not provide individuals with a generally recognised digital identity but has endorsed the digital identity card provided by the UK non-profit scheme CitizenCard Limited, which can be used to self-identify online (or physically).

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

Guernsey collective investment schemes are regulated under the POI Law and are required to be administered by a Guernsey-licensed administrator. Additionally, open-ended funds are usually required to custodise their assets with a Guernsey-licensed custodian. The definition of collective investment scheme sets out four characteristics that must be met for an entity to comprise a collective investment scheme. These are:

a the vehicle involves pooling of investors’ money for investment in a common portfolio (‘Spread of Investors’); \(^6\)

b the common portfolio holds assets intended to spread risk (‘Spread of Risk’); \(^7\)

c there is no intention to exercise day-to-day management control over any business in which the vehicle invests; \(^8\)

d the portfolio is managed by a professional manager, at arm’s length from the investors in the collective investment scheme (this is covered by (c) and (d), together referred to as ‘Independent Management’). \(^9\)

In short, a structure is likely to be a collective investment scheme for the purposes of the POI Law where there is a Spread of Investors, a Spread of Risk and Independent Management.

Investing in cryptocurrencies, ICOs or both is possible for collective investment schemes; however, the GFSC have emphasised the perceived volatility of this asset class and will expect collective investment schemes operating in the space to have adequate controls in place to address this.

All collective investment schemes in Guernsey are required to have in place a Guernsey-licensed fund administrator. For open-ended schemes, a Guernsey-licensed custodian is also required although alternative custody arrangements may be approved by the GFSC where the assets involved make this appropriate.

Crowdfunding and crowd-lending are both permitted, as is peer-to-peer lending. All three structures are likely to fall within one of the categories defined as a financial services business for the purposes of the NRFSB Law and require registration. Guernsey does not have any consumer lending regulation in place (although there is a long-standing but rarely utilised prohibition dating to the 1930s on the charging of excessive interest, likely only to apply where the interest is owed by an individual). \(^10\)

A consultation was commenced in 2017 around revised regulation in respect of lending, credit and finance regulation in Guernsey – the proposals would involve the replacement of

---

\(^6\) Paragraph 1(1)(c)(i) of Schedule 1 to the Pol Law.
\(^7\) Paragraph 1(a) of Schedule 1 to the Pol Law.
\(^8\) Paragraphs 1(1)(b) and 1(1)(c)(ii) of Schedule 1 to the Pol Law.
\(^9\) Paragraph 1(c)(ii) of Schedule 1 to the Pol Law.
\(^10\) The Ordonnance Donnant Pouvoir à La Cour de Réduire Les Intérêts Ecessifs, 1930.
the NRFSB Law and regulation around consumer lending and credit. A core goal of this consultation was ensuring consumer interests were matched with the ability for Guernsey companies to operate internationally. Noted among the responses to the consultation was industry ‘encouragement to implement a framework that portrays a positive approach towards progressing advances in the use of technology and the digital sector’. Development of legislation in respect of this consultation is ongoing and is likely to form part of the Guernsey government’s stated intention to continue to develop the Fintech sector in Guernsey.

Operating an investment exchange is a restricted activity in Guernsey under the POI Law. To the extent businesses permit trading in loans or financing on a secondary market (or unitise or securitise those loans and permit trading in those), consideration should be given to whether an investment exchange is being created. To the extent that what is being transferred or offered meets the POI Law definition of a general security or derivative, consideration should also be given as to whether any other restricted activity (promotion or advising for example) is being undertaken that would trigger a licensing requirement.

Payment services operations are also unlicensed and again typically require registration under the NRFSB Law to ensure suitable AML and CFT procedures are in place.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

There is no specific regulation of blockchain technology, which is increasingly being used in the broader regulated financial services sector in Guernsey. In February 2017, Northern Trust in Guernsey, in collaboration with IBM, launched the first commercial deployment of blockchain technology for the private equity market – a distributed ledger solution used for the management and administration of a private equity fund by Unigestion, a Swiss-based asset manager with US$20 billion assets under management. This use of blockchain was launched following the approval of the GFSC.

Guernsey insurance businesses have also utilised the blockchain – Solidum Partners utilises the private ILSBlockchain to create, settle and permit transfers of catastrophe bonds issued by its Guernsey-based transformer, Solidum Re (Guernsey ICC) Limited.

Basic anti-money laundering laws apply to all businesses operating in Guernsey. These laws create a series of obligations and offences around disclosure to the Financial Intelligence Unit if knowledge or suspicion of money laundering or terrorist financing arises (or where an individual has reasonable grounds for such suspicion).

More specific anti-money laundering rules apply to Guernsey companies and businesses that are captured within the Guernsey regulatory regime. For the purposes of this chapter, those are primarily those companies carrying on activities requiring a licence under Guernsey’s financial services regulatory regime or the NRFSB Law.

To the extent that such a business falls outside the licensing regime of the POI Law, it will almost certainly be captured by one of the heads of business set out in the NRFSB Law (notably, operating a money service business, facilitating or transmitting money or value or issuing, redeeming, managing or administering means of payment). As previously noted,

12 Paragraph 4, Schedule 1 Part 1, NRFSB Law.
13 Paragraph 5, Schedule 1 Part 1, NRFSB Law.
14 Paragraph 6, Schedule 1 Part 1, NRFSB Law.
the extent to which the POI Law licensing obligations will apply in the cryptocurrencies or ICO space will depend upon the extent to which the assets in question constitute ‘general securities and derivatives’, as that term is defined in Category 2 of Schedule 1 of the POI Law and is likely to come down to a factual analysis of each situation.

VI OTHER NEW BUSINESS MODELS

Guernsey has had an electronic transactions law in place (providing for the electronic execution of contracts) since 2000.\textsuperscript{15} At the time of writing a new ordinance is in the process of being passed (and is expected to be in force by the time of publication), which will clarify that:

\begin{itemize}
  \item[a] the formation, execution, performance or termination of a contract shall not be denied legal effect solely because it involved the action of one or more electronic agents;
  \item[b] contracts may be formed by the interaction of electronic agents (without input from natural persons); and
  \item[c] contracts may be formed by the interaction of an electronic agent and a natural person.
\end{itemize}

An ‘electronic agent’ is defined in The Electronic Transactions (Guernsey) Law 2000 as:\textsuperscript{16}

\begin{quote}
  A computer program or electronic or other automated means used independently to initiate an action or to respond in whole or in part to information or actions in electronic form or communicated by electronic means, without review or action by a natural person.
\end{quote}

As such, the use of ‘smart’ contracts and other self-executing mechanisms derived using artificial intelligence or algorithms is fully recognised under Guernsey law.

Funds utilising fully automated investment processes have been approved by the GFSC. In this situation, the regulator will expect there to be sufficient oversight of the algorithm or automation to ensure investors are suitably protected. Responsibility for this oversight rests with the board of a licensee, and the GFSC is expected to apply this approach to any use of artificial intelligence by a licensee. The GFSC has been clear that its expectations of board members on technology issues are that they need to engage with and understand any use of technologies by their businesses to understand the limitations and risks therein, and ensure proper human oversight of those risks.

Third-party websites comparing products or providing information about financial products would be subject to the Data Protection (Bailiwick of Guernsey) Law 2017 (DPGL) regime detailed below to the extent they were operating in Guernsey and dealing with the data of individuals. The POI Law (and other financial services laws depending on the product offered, for example, insurance) may also apply to the extent the website constituted promotion or the offering of a product for sale in or from within Guernsey.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Guernsey has a robust and extensive suite of intellectual property laws, including certain rights not available in many other jurisdictions.

\textsuperscript{15} The Electronic Transactions (Guernsey) Law 2000.

\textsuperscript{16} Section 14(3), the Electronic Transactions (Guernsey) Law 2000.
Potentially of particular relevance to fintech business models is the Guernsey database right. In Guernsey (in addition to any copyright subsisting in a database), databases are protected under the Database Rights (Bailiwick of Guernsey) Ordinance 2005 (the Database Ordinance).

A database is defined under the Database Ordinance as ‘a collection of independent works, data or other materials which (a) are arranged in a systematic or methodical way, and (b) are individually accessible by electronic or other means’, a wide definition covering a range of data-holding structures. A database right protects the compilation of information comprising the data and subsists where there has been a substantial investment in the collation of the contents of the database.

Database rights, like other property rights, can be sold, licensed or assigned to third parties. A database is often a valuable asset that businesses are increasingly looking to exploit in their own right.

Similar to copyright, a database right is an automatic right and subsists from the moment the database is created in a recorded form. Database rights last for a period of 15 years from the end of the calendar year in which the database was completed. Where a database is made available to the public before the end of the 15-year period, the protection period will be extended by a further 15 years from the end of the calendar year in which it was first made publicly available. Additionally, if there is a substantial change to the contents of the database then the 15-year protection period recommences. In effect, this means that an indefinite term of protection is available for many databases that are continually updated.

Other more typical intellectual property rights and protections such as copyright, patents and trademarks are all also available in Guernsey as well as the world’s first registerable image right. Typically, Guernsey intellectual property laws provide a presumption that intellectual property rights developed by an employee in the course of their employment belong to the employer (this is the case for patent, copyright and database rights, among others) subject to rebuttal by reference to specific factual differences.

From a data protection perspective, Guernsey is one of a small number of jurisdictions historically deemed to have an equivalent data protection regime to the European Union. To maintain this status following the General Data Protection Regulation, the DPGL was enacted.

The DPGL deals with duties of data controllers (including the data protection principles), duties of data processors, conditions for processing, obligations to appoint data protection officers, rights of data subjects, exemptions to parts of the law, cross-border transfers and exemptions to the adequacy requirements and remedies and enforcement. The DPGL largely mirrors the EU position and the rules around digital profiling are similar to those in the EU.

The DPGL established the office of the Data Protection Authority in Guernsey, and includes powers allowing it to investigate complaints and undertake inquiries along with granting it powers of sanction following a finding of a breach (including fines). Owing to the similarity of Guernsey law to EU law in this area, the approach of the Data Protection Authority in Guernsey in enforcing the law and treatment of certain technologies and uses of

---

17 Section 54, the Registered Patents and Biotechnological Inventions (Bailiwick of Guernsey) Ordinance 2009.
18 Section 12(1), the Copyright (Bailiwick of Guernsey) Ordinance 2005.
19 Section 4(2), the Database Rights (Bailiwick of Guernsey) Ordinance 2005.
data (such as profiling) is likely to be similar to that employed by European data protection regulators (and indeed the UK Information Commissioner’s Office post-Brexit). European case law and enforcement actions will likely be influential.

**VIII YEAR IN REVIEW**

From a Guernsey perspective, the most significant aspect of the past year has been the formal identification of fintech as one of the keys for the ongoing development of Guernsey’s financial services industry, in the States of Guernsey and Guernsey Finance’s ‘Financial Services Policy Framework’.

The focus on financial technologies (notably in the areas of electronic due diligence and distributed ledger technologies) in the Policy Framework makes clear that creating an enabling environment for businesses looking to use fintech is a core objective of both the local financial services industry and the government. Arising out of this overall strategic direction have been a number of developments in the law and regulation around fintech, notably the changes to the AML handbook around electronic due diligence and the approval of clarificatory legislation around electronic transactions.

While no individual change has been groundbreaking, and we have not seen the enactment of legislation directly aimed at fintech specifically, these smaller enabling changes are indicative of an approach to fintech that looks to enable its use and development by Guernsey’s established financial services industry. Arising out of this, we have also seen the GFSC work with industry to facilitate the use of a range of disruptive technologies within industry, and this engagement has been received very positively by industry.

**IX OUTLOOK AND CONCLUSIONS**

We expect to see continued growth in Guernsey’s fintech sector over the forthcoming year. In our view, much of this growth will come from the application of financial technologies to traditional business models.

Specifically, we expect to see continued growth in the use of blockchain for private equity transactions and other investment asset exchanges, as well as the expansion of the use of digital onboarding of clients by investment funds, fiduciary service providers and local banks. We also anticipate the expanded use of artificial intelligence in Guernsey financial services (subject to appropriate human oversight).

As regards cryptocurrencies and ICOs, we expect primarily to see these used as investment assets by structures based in Guernsey rather than structures or assets launched out of Guernsey in their own right (as has been the case to date).

At this time we are unaware of plans for significant legislative change that would directly impact the fintech sector (with the possible exception of consumer credit legislation). However, it is to be expected that updates to existing laws will continue to be made in a way that enables the use of financial technologies wherever possible.
Chapter 9

HONG KONG

Yu Pui Hang (Henry Yu)\(^1\)

I OVERVIEW

Benefiting from its low tax rates, the ‘one country, two systems’ principle and its proximity to mainland China, Hong Kong is one of the biggest international financial centres in the world, and attracts businesses from all around the world that are interested in tapping into the Chinese market and vice versa. With the rapid development of and increased appetite for technology in the financial sector, Hong Kong is well poised to take advantage of the opportunities brought about by the development of the Greater Bay Area, and continues attract businesses from all around the world that are interested in participating in the fintech sector.

As of time of writing, Hong Kong remains largely technologically neutral with regard to technological development in the financial sector. Hong Kong regulatory bodies remain cautious: they generally apply the existing regulatory framework to technological developments (e.g., to use the current legislation regarding securities to attempt to regulate cryptocurrency exchanges) and issue guidance regarding the latest hot topics from time to time (e.g., position papers and guidelines regarding the regulation of cryptocurrency, digital payments). Otherwise, Hong Kong generally welcomes technological advancements and will likely continue to adopt this attitude in the foreseeable future. Hong Kong authorities have granted multiple licences encompassing multiple facets of the fintech sector, including eight virtual bank licences, two virtual insurer licences, 18 stored value facility licences and several automated digital advising licences.

II REGULATION

i Licensing and marketing

There are several licences that are applicable to the fintech industry, depending on the business being conducted by a corporation, but there is no one specific licence for fintech, in light of the broad spectrum of services available in this field. These include: (1) the virtual bank licence, issued by the Hong Kong Monetary Authority (HKMA), which allows the licence holder to deliver retail banking services through the internet instead of a physical branch; (2) the stored-value facility licence, also issued by the HKMA, which governs the operation of retail payment systems and stored value facilities; (3) various securities licences, issued by the Securities and Futures Commission (SFC), which allow the holder to carry out regulated

---

\(^{1}\) Yu Pui Hang (Henry Yu) is the principal partner at Henry Yu & Associates, in association with L & Y Law Office.
activities (most likely covering services that involve securities and futures); (4) the money service operator licence (MSO), issued by the Customs and Excise Department (CED), which allows licence holders to provide money services; and (5) the money lender’s licence, issued by the Hong Kong court and monitored by the Hong Kong Police (which allows a person to carry out business as a money lender in Hong Kong). With the increasing popularity of ‘insurtech’ (which falls under the umbrella of fintech), the Insurance Authority may also issue relevant insurance licences if the product being handled relates to an insurance product.

Depending on the exact nature and scope of regulated activities to be carried out by such a corporation, provision of an automated digital advisory service typically requires a licence from the SFC to carry out Type 1 (dealing in securities) and Type 4 (advising on securities). A corporation providing asset management services would typically require a licence from the SFC to carry out Type 4 (advising on securities) and Type 9 (asset management) regulated activities.

Credit information services are generally governed by Type 10 regulated activities (providing credit ratings services) under the Securities and Futures Ordinance (SFO), pursuant to which ‘credit ratings’ are defined as opinions, expressed using a defined ranking system, primarily regarding the creditworthiness of: (1) a person other than an individual; (2) debt securities; (3) preferred securities; or (4) an agreement to provide credit. Corporations carrying out such regulated activities would also be required to comply with the Code of Conduct for Persons Providing Credit Rating Services issued by the SFC in June 2011.

Under the Companies (Winding Up and Miscellaneous Provisions) Ordinance (CWUMPO), it shall not be lawful to issue any form of application for shares in or debentures of a company to the Hong Kong public unless the form is issued with a prospectus that complies with the requirements of the CWUMPO and is registered with the Registrar of Companies in Hong Kong (the Prospectus Requirements). In addition, Section 103 of the SFO prohibits a person from issuing an advertisement, invitation or document which to his knowledge is or contains an invitation to the public to deal in any ‘securities’ (which is widely defined under Schedule 1 to the SFO) unless the issue has been authorised by SFC (the SFC Authorisation), which will in turn require the offering document to comply with the Prospectus Requirements. There are certain exemptions to the Prospectus Requirement and the SFC Authorisation requirement, the most common of which are:

a. professional investors exemption: offers made to professional investors only (as defined under the SFO);
b. private placement exemption: offers made to a maximum of 50 persons in Hong Kong provided that the offering document contains a warning statement as specified under Part 3 of Schedule 18 to the CWUMPO;
c. sophisticated investor exemption: offers where the minimum principal amount to be subscribed by any person is not less than HK$500,000 (or its foreign currency equivalent), with the appropriate specified warning statement in a prominent position of the offering document;
d. de minimis offering exemption: offers in respect of which the total considerable payable for the offering does not exceed HK$5 million (or its foreign currency equivalent); and
e. outside HK investors exemption: offers to persons outside Hong Kong.

2 e.g., Chloe by 8 Securities Limited and Aquamon by Magnum Research Limited, both of which have obtained Type 1 (dealing in securities) and Type 4 (advising on securities) licences.
3 e.g., Kristal.AI by Kristal Advisors (HK) Limited, has obtained Type 4 (advising on securities) and Type 9 (assessment management) licences.
Section 114 of the SFO also prohibits carrying on a business in a regulated activity, or holding oneself out as doing so, save for a licensed intermediary or an authorised institution. In addition, pursuant to the Code of Conduct for Persons licensed by or Registered with the Securities and Futures Commission (the SFC Code of Conduct), licensed intermediaries are required to act honestly and fairly towards customers. Paragraph 2.3 of the SFC Code of Conduct further requires licensed intermediaries to ensure that invitations and advertisements do not contain information that is false, disparaging, misleading or deceptive. The SFC has also issued guidelines including but not limited to the Advertising Guidelines Applicable to Collective Investment Schemes Authorised under the Product Codes, Guidelines on Use of Offer Awareness and Summary Disclosure Materials in Offerings of Shares and Debentures Under the Companies Ordinance and Guidelines on Marketing Materials for Listed Structured Products (collectively, the SFC Marketing Guidelines), all of which will apply to various forms of product advertisements (e.g., distribution materials, display-only materials, broadcasts and interactive systems). For illustration purposes, in the case of collective investment schemes, the material must: (1) not be false, biased, misleading or deceptive; (2) be clear, fair and present a balanced picture of the scheme with adequate risk disclosures; and (3) contain information that is timely and consistent with its offering document. The SFC Marketing Guidelines have also imposed requirements on the content of the material, such as requiring statements of opinion regarding a structured product or management company’s level of performance to (1) be reasonable; (2) not contain words or phrases that may give investors the impression that they cannot lose money or that profits are guaranteed (unless the scheme has a guarantee feature); (3) not give the impression that an investor could profit without risk; and (4) not seek to denigrate competitors in such a way as might lower the reputation of the industry. There are also requirements that are specific to other medium of marketing, including radio, television, cinema or other time-limiting advertisements or broadcasts to reinforce marketing may only be conducted if there are sufficient investor protections in place.

If a corporation operates an automated digital advisory or asset management company relating to financial products or services, it may also be bound by additional guidelines issued by the SFC – the Guidelines on Online Distribution and Advisory Platforms issued in July 2019 (the SFC Online Guidelines). Among other principles, the platform operator should comply with the six core principles identified by the SFC, including (1) proper design; (2) information for clients; (3) risk management; (4) governance, capabilities and resources; (5) review and monitoring; and (6) record keeping. If such a corporation is to provide robo-advice, a service by which advice is provided directly to clients online through the direct use of technology tools by clients, Chapter 4 of the SFC Online Guidelines would apply. According to these, the robo-advisor should comply with various rules regarding the provision of sufficient information to clients, client profiling, system design and development, supervision and testing of algorithms, adequate resources and rebalancing outlined in the SFC Online Guidelines.

ii Cross-border issues

As a general rule, if a corporation deals with the general public in Hong Kong, their activities would be subject to Hong Kong law. If the services or products provided by such corporations are securities related, such services or products would be governed by the SFO. The SFO is silent on whether the regulated activities are subject to any geographical requirements, but it is generally interpreted that a foreign corporation may still be subject to Section 103 of the
SFO if it has marketing activities in Hong Kong. Whether there is any active marketing in Hong Kong would be determined by the specific circumstances (for example, whether the corporation had contacted a Hong Kong investor or organised events targeting Hong Kong investors). If it is determined that a foreign corporation is marketing in Hong Kong, they may need to be licensed or registered with the SFC and may even be subject to the Prospectus Requirements and the SFC Authorisation requirement under the the Companies Ordinance and the SFO, unless one of the exemptions discussed above applies.

To the extent of fund distribution, following memoranda of understanding (MOUs) signed by Hong Kong with China, Switzerland, France, Luxembourg and the United Kingdom, a system of mutual recognition of funds is put in place between Hong Kong and the above-mentioned signing countries to allow eligible funds to be passported into Hong Kong and vice versa. The MOUs with each country differ slightly from each other on the structure of the funds and the type of funds that would be eligible for mutual recognition. For example, the MOU with France requires the fund to retain a minimum of 20 per cent of the net asset value to be attributable to Hong Kong investors, the MOU with the United Kingdom prohibits leverage over 100 per cent of the net asset value, and the MOU with Luxembourg requires the fund to be managed by a fund manager who has a minimum of HK$10 million in capital. Having said that, all foreign funds to be offered into Hong Kong will require the fund to appoint a firm in Hong Kong as representative and also engage a licensed intermediary to carry out any marketing activities of the fund in Hong Kong.

Similarly, under Section 114 of the SFO, the restriction on carrying on business in regulated activities does not make any distinction between foreign or local corporations. Therefore, corporations should obtain licences from the SFC if they provide cross-border regulated services and products targeting the Hong Kong public.

Nevertheless, a temporary licence under Section 117 of the SFO could be available to foreign corporations if they are already licensed or regulated in other jurisdictions. Such temporary licence, if granted, is valid for up to three months, and the same person cannot hold a temporary licence for more than six months in any two-year period. The SFC will consider whether the foreign corporation is subject to similar regulatory requirements as imposed, monitored or enforced by the foreign corporation’s local regulator and whether such local regulator would be able to take disciplinary action against the foreign corporation for their actions in Hong Kong as part of the consideration in granting the temporary licence. There are also other restrictions to the temporary licence, such as not allowing all types of regulated activities or not holding all client assets.

The restrictions relating to offering or inviting investors under Section 103 of the SFO are only relevant to invitation to investments made in Hong Kong, but there is no specific restriction under the SFO if there is a genuine enquiry made by a Hong Kong investor to the foreign corporation. Provided that the response to the enquiry made by the Hong Kong investor is bespoke and tailored to the enquiry, the foreign corporation may not be subject to the restriction under Section 103. This is a process that is commonly referred to as ‘reverse enquiry’.

There are no currency exchange controls in Hong Kong, but the flows of funds in and out of Hong Kong may be prohibited or restricted by laws such as United Nation (Anti-Terrorism Measures) Ordinance, United Nations Sanctions Ordinance and other relevant laws and regulations. There is no limitation on ownership of companies by foreigners in place in Hong Kong.
III DIGITAL IDENTITY AND ONBOARDING

There are no laws and regulations in Hong Kong relating to establishing digital identity but a similar concept was introduced by the Electronic Transaction Ordinance (ETO), which allows digital certificates to be created to serve as a guaranty of identity during electronic transactions. Digital certificates can only be issued by recognised certification authorities, which to this date only include the Hongkong Post Certification Authority and Digi-Sign Certification Services Limited. Nevertheless, any person may apply to the Government Chief Information Officer to become a recognised certification authority pursuant to Section 20 of the ETO. Once issued, digital certificates can be used to identify a person in a process known as electronic authentication to verify transactions. At the moment, personal digital certificates can only be applied by individuals who possess a Hong Kong identity card (the applications do not accept other form of identification documents, such as passports). On the other hand, corporations can also apply for digital certificates and there is no restriction on the jurisdiction of the corporations as long as the corporation has obtained a business registration certificate issued by the Hong Kong government.

The ETO covers situations when electronic signature or services can be used, including transactions between private individuals or with government entities. Digital certificates are more commonly used for any applications or transactions with government entities, for example, voter registration and applications for renewal of vehicle licences. The ETO also recognises private transactions conducted by electronic means provided the parties to the transaction consent to it. Pursuant to ‘Supplement V to the Mainland and Hong Kong Closer Economic Partnership Arrangement’ (CEPA) and the Suggestions on the Framework for the Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong, a mutual recognition arrangement and the mutual recognition certificate policy was developed and entered into on 10 August 2012, pursuant to which digital certificates issued by the recognised certification authority in Hong Kong are mutually recognised in the Guangdong province of China and vice versa, provided that the authorisation of the recognised certification authority and its conduct observes and complies with the mutual recognition certificate policy.

Pursuant to the amended Paragraph 5.1 of the SFC Code of Conduct (which took effect on 5 July 2019), acceptable account opening methods are now set out in the SFC’s website instead of in the SFC Code of Conduct. The SFC also issued the Circular to Intermediaries: Remote Onboarding of Overseas Individual Clients on 28 June 2019, along with an FAQ to address various issues regarding digital onboarding. In addition to the face-to-face approach, the SFC now permits a licensed intermediary to adopt other account opening procedures, provided that such procedures can satisfactorily ensure the identity of the client. There are several methods that are acceptable according to the SFC: (1) certification by another person (whereby a client agreement and the identity documents of the customer are being certified by another licensed person, an affiliate, a Justice of the Peace or a professional person); (2) using the certification services (when the licensed intermediary accepts an electronic signature certificate to replace actual identity documents); (3) by mail (where the customer mails a copy of the identity document and the client agreement to the intermediary together with a physical cheque bearing the same signature as the one on the client agreement); (4) online onboarding with a Hong Kong designated bank account (where the customer electronically signs the client agreement and provides a copy of the identity document, and all future deposits and withdrawals from the client’s trading account must be with a bank account in Hong Kong in the customer’s name); and (5) remote onboarding of overseas individual
clients (where technology adhering to the international standards and best practice such as ISO/IEC 19795 (biometric performance testing and reporting) and ISO/IEC 30107 (biometric presentation attack detection) are adopted in the process of client identification together with requiring all deposits into and withdrawals from the client’s trading account be with a bank account opened with a designated bank in the customer’s name from an eligible jurisdiction). For point (5), there are currently 16 eligible jurisdictions, namely Australia, Austria, Belgium, Canada, Ireland, Israel, Italy, Malaysia, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, the United Kingdom and the United States.

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

The SFC issued the Position Paper: Regulation of Virtual Asset Trading Platform (the Position Paper) on 6 November 2019 announcing that ‘some types of centralized platforms trading security and non-security tokens would be suitable to be regulated’ by the SFC with the regulatory standards similar to those required of licensed automated trading service (ATS) providers or brokers.

The SFC has reiterated in the Position Paper that platform operators that trade only non-security virtual assets are not regarded as carrying out ‘regulated activities’ for the purposes of the SFO, and these platform operators may continue to operate in Hong Kong without applying for an SFC licence. Nevertheless, if a platform operator decides to opt in to the SFC regulatory remit, which would require the platform operator to offer at least one security token on its platform, the SFC would be empowered to grant the licences for Type 1 (dealing in securities) and Type 7 (providing ATS). The SFC will take a holistic approach to the infrastructure, core fitness and properness and conduct of all virtual assets (be they securities or not) trading activities viewed as a whole and subject to the SFC’s supervision.

If the SFC decides to grant the licences (Types 1 and 7) to a platform operator, it will impose certain licensing conditions that are outlined in the terms and conditions attached to the Position Paper. The licensed platform operator is also required to comply with all other regulatory requirements as set out in the SFC Code of Conduct and Guidelines, circulars and frequently asked questions published by the SFC from time to time. It is important to note that any breach of the above could be considered ‘misconduct’, which may also reflect adversely on the fitness and properness of a licensed platform operator and may result in disciplinary action including licence revocation and fines. Despite the innovative approach by the SFC to virtual assets platform operators, there remain certain limitations on the SFC’s regulatory power over virtual assets platform operators and their licensed platforms. For example, whether the SFC is able to take action under Parts XIII and XIV of the SFO against market misconduct on such platforms in the same way it does in the traditional securities and futures market remains to be seen.

Section 103 of the SFO prohibits the advertisement of offers and invitations to participate in a ‘collective investment schemes’ (CIS) unless one of the exemptions applicable to the Prospectus Requirement and SFC Authorisation, as referred to above under the Section ‘Regulation’, applies. A CIS is defined in Paragraph (d) of the definition of ‘securities’ of Schedule 1 of the SFO, which includes interests in ‘collective investment schemes’. A CIS is an investment product that is collective in nature, the definition embraces and modernises the concepts of ‘unit trust’, ‘mutual fund corporation’ and ‘investment arrangements’. The definition under Schedule 1 can be narrowed down to a more concise four-part test: a collective investment scheme generally requires: (1) an arrangement in respect of property;
that participants in the scheme do not have day-to-day control over the management of the property; (3) such property is managed as a whole by or on behalf of the person operating the arrangements, or the contribution of the participants and the profits or income from which payments are made are pooled; and (4) the purpose of the arrangement is for participants to participate in or receive profits, income or other returns from the acquisition and management of property.

Hong Kong does not have any specific laws or regulations in relation to crowdfunding. Crowdfunding activities such as peer-to-peer lending in Hong Kong and equity crowdfunding may be considered as a CIS and, if offered to the public in Hong Kong, may be subject to a number of Hong Kong regulatory provisions, for example, the Prospectus Requirement and the SFC Authorisation requirement unless an exemption applies (see Section II).

Operators of crowdfunding platforms would also be subject to Section 103 of the SFO as outlined above. If the operator of a crowdfunding platform carries on a regulated activity, it is required to obtain appropriate SFC licences and would also be required to comply with the SFC Code of Conduct, which contains provisions requiring licensed intermediaries to establish clients’ financial situations, investment experience and ensure that investment products recommended to the clients are suitable.

In addition to the same regulatory prohibitions that may be applicable to crowdfunding as outlined above, peer-to-peer lending by individuals or businesses might constitute the carrying on of business as a money lender, which requires the person or business to be a licensed money lender under the Money Lenders Ordinance (MLO). The MLO requires anyone who wishes to carry on business as a money lender to apply to a licensing court for a licence, processed by the Companies Registry and enforced by the Commissioner of Police. The term ‘money lender’ is defined in Section 2 of the MLO as ‘every person whose business (whether or not he carries on any other business) is that of making loans or who advertises or announces himself or holds himself out in any way as carrying on that business’. Certain persons and loans under Schedule 1 of the MLO are excluded from the definition. Peer-to-peer lenders may be able to rely on an exemption where the corporation, firm or individual making the loan does not carry out the lending of money as its ordinary business. It would, however, be difficult in the case of any individual lender to determine at what point the lender is ‘carrying on a business of lending money’.

Subject to whether the loans or financings would constitute securities (which is inclusive of an interest in a CIS), trading of such loans or financings may fall under the regulation of the SFO, which means only licensed corporations can conduct any secondary trading. Otherwise, transfers of loans and financings may be conducted by way of legal or equitable assignment:

Legal assignment: a legal assignment is an assignment which meets the criteria set out in the Law Amendment and Reform (Consolidation) Ordinance:

- an absolute assignment by way of sale of the assignor’s entire legal interest in the receivables (e.g. loan);
- in writing and signed by the assignor; and
- with express written notice of the assignment (in particular the date of assignment and the identity of the assignee) given to the obligor.

© 2020 Law Business Research Ltd
Equitable assignment: an equitable assignment is an assignment that has not met all the requirements as mentioned to create a legal assignment (typically, not being able to give notice to the obligor).

In Hong Kong, there are no laws specifically for securitisation other than in respect of capital treatment and disclosure requirements for ‘authorised institutions’ as defined in the Banking Ordinance (BO) (e.g., banks).

Any person operating a money service should be licensed with the Commissioner of Customs and Excise pursuant to the Anti-Money Laundering and Counter Terrorist Financing Ordinance (AMLO). ‘Money service’ includes money changing and remittance services.

If the person operating the payment service issues a facility that can store value and gives an undertaking that such facility may be used for the payments for goods or services of either the issuer or another person, the person may be required to be licensed with the stored-value facility licence (the SVF licence) pursuant to the Payment Systems and Stored Value Facilities Ordinance (PSSVFO). The ‘undertaking’ referred to above means an undertaking that the issuer will accept payment up to the amount of the stored value that is available for use under the rules of the facility or that the issuer will make payment to the recipient of such amount. It is noteworthy that the SVF licence also applies to a ‘facilitator’, which is defined to be anyone who is not the issuer and provides the issuer with valuable consideration the value of which determines the extent to which the issuer may give an undertaking (for example, by providing the reserve in some of the business model (of ‘stablecoins’).

Businesses in Hong Kong are subject to the Personal Data (Privacy) Ordinance (PDPO), which regulates the collection, use and handling of personal data received by corporations or persons (the data users). PDPO places restrictions on use and disclosure of personal data under Data Protection Principle 3 of the PDPO and thus data users should not make client data accessible to third parties without the consent of the client under normal circumstances.

However, the PDPO also contains exemptions to the restrictions on use and disclosure of client data under Data Protection Principle 3. Exemptions apply for any use or disclosure of client data which is (1) required or authorised by any Hong Kong law or court order; (2) required in connection with legal proceedings in Hong Kong or exercising or defending legal rights in Hong Kong; (3) for the purpose of a due diligence exercise in connection with a proposed sale or merger; and (4) for the purpose of preparing statistics or carrying out research (provided that no identifying information of any client is published).

In relation to product data, companies would need to disclose its product data if it is requested by a regulator in Hong Kong to provide such information in accordance with the provisions of a specific law in Hong Kong. There are various laws in Hong Kong that grant wide investigative powers to authorities in Hong Kong to conduct investigations, including the SFC, HKMA, the Insurance Authority and the Hong Kong Independent Commission against Corruption (ICAC).
V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

There is no specific regulatory framework for blockchain technology in Hong Kong. Such technology and related businesses are subject to the existing body of Hong Kong financial laws and regulations. However, the HKMA and the SFC have issued a number of statements clarifying their regulatory stance.

In February 2015, HKMA stated in a press release that Bitcoin is not legal tender but a virtual commodity. Given that Bitcoin does not have any backing, either in physical form or from the issuer, it cannot be qualified as a means of payment or electronic money. The HKMA expressly stated that it does not regulate Bitcoin and other similar virtual commodities.

The SFC issued a statement on 5 September 2017 (the 2017 Statement), addressing the issue of initial coin offerings (ICO). Offering cryptocurrencies to investors in Hong Kong (as part of an ICO) may, depending on the feature of the ICO, be subject to Hong Kong’s existing securities law regime. The 2017 Statement outlines specifically three types of terms and features of digital tokens in ICOs that might constitute securities:

- Tokens may be regarded as shares if they represent equity or ownership interests in a corporation, for example, where the token holders are given shareholders’ rights, including the right to receive dividends and the right to participate in the distribution of the corporation’s surplus assets upon winding up.
- Tokens may be regarded as debentures where the digital tokens are used to create or to acknowledge a debt or liability owed by the issuer. For example, an issuer may repay token holders the principal of their investment on a fixed date or upon redemption, with interest paid to token holders.
- Tokens may be regarded as an interest in a CIS if the token proceeds are managed collectively by the ICO scheme operator to invest in projects with the aim of enabling token holders to participate in a share of the returns provided by the projects. The concept of CIS has been set out under Section IV.

The SFC published a circular in December 2017 in relation to Bitcoin futures contracts and other cryptocurrency-related investment products, where the SFC warned that Bitcoin futures contracts traded on a futures exchange are regarded as ‘future contracts’ for the purposes of the SFO, even though the underlying assets of such future contracts may not be regulated under the SFO. It was noted that other cryptocurrency-related investment products may, depending on their terms and features, be regarded as ‘securities’ as defined under the SFO.

In November 2018, the SFC issued the Statement on Regulatory Framework for Virtual Asset Portfolios Managers, Fund Distributors and Trading Platform Operators (the 2018 Statement). The Statement introduced the concept of a new asset class called ‘virtual assets’, which are ‘a digital representation of value’. Examples include cryptocurrencies, cryptoassets and digital tokens (such as digital currencies, utility tokens or security or asset-backed tokens) and any other virtual commodities, cryptoassets and other assets of essentially the same nature. The SFC has not made clear which tokens or coins would fall under this new asset class but has admitted that many virtual assets do not necessarily constitute securities or futures contracts for the purpose of the SFO.

The 2018 SFC issued a statement on 28 March 2019 that further confirms the SFC’s approach to virtual assets which fall within the definition of ‘securities’ under the SFO (security tokens) and confirms that marketing and distribution of security tokens must be conducted by a person licensed and registered for Type 1 regulated activity (as further set out
The SFC places substantial reliance on Type 1 intermediaries to comply with the existing codes of conduct, new guidance issued by the SFC and other laws and regulations, to ensure that purchasers of security tokens are fully protected. This includes restricting the offerings of security tokens to professional investors only, conducting thorough due diligence on the security tokens and the issue of such tokens, the asset backing the security tokens and all other relevant materials, and providing all information to the purchaser in a clear and easily comprehensible manner.

The SFC has emphasised the importance of compliance with the suitability requirement in Paragraph 5.2 of the SFC Code of Conduct, as well as the new requirements for ‘complex products’ in Paragraph 5.5 of the SFC Code of Conduct, which came into effect on 6 July 2019.

The SFC has also highlighted key requirements of its Circular to Intermediaries on the Distribution of Virtual Asset Funds dated 1 November 2018 (that would apply equally to the distribution of security tokens):

a. Security tokens should only be offered to persons who qualify as ‘professional investors’ under the SFO and the Securities and Futures (Professional Investor) Rules.

b. Intermediaries distributing security tokens need to understand the STOs and conduct proper due diligence, covering the background and financial soundness of the management, development team and issuers of the security tokens as well as the rights attached to the underlying assets of the security tokens. Intermediaries should also review the White Papers and marketing materials in respect of the STOs.

c. Intermediaries should give clients information relating to STOs in a clear and easily comprehensible manner and should give clients prominent warning statements covering the risks associated with virtual assets. These risks include insufficient liquidity, volatility, opaque pricing, hacking and fraud.

Tokens can be linked to the underlying assets through recording the asset digitally and provide a graphically secured representation of value that can be stored and transferred within a distributed ledger.

The current system in Hong Kong requires the issuance of paper certificates and use of paper instruments of transfer for certain securities. Under Section 144 of the Companies Ordinance (CO), a company must complete and issue share certificates after an allotment of shares has been completed. Nevertheless, there have been movements toward paperless securities regime in Hong Kong over the last two decades. The Securities and Futures and Companies Legislation (Uncertificated Securities Market Amendment) Ordinance 2015 (the Amendment Ordinance) includes provisions introducing an uncertificated securities market regime (therefore paperless). However, as of the date of this article, the Amendment Ordinance is not yet in effect.

There are no laws and regulations that specifically deal with the laundering of cryptocurrencies and tokens. The Anti-Money Laundering Ordinance (AMLO) principally applies to financial institutions (including HKMA-authorised institutions (i.e., banks, SFC-licensed corporations, licensed insurance companies, stored-value facility issuers and money service operators) and designated non-financial business and professions (DNFBP) (e.g., law firms). If a corporation deals with cryptocurrencies and tokens, it is not directly subject to the provision of the AMLO, unless such corporation falls within the definition of financial institutions or DNFBPs.
In addition to the AMLO, corporations would be subject to the Drug Trafficking (Recovery of proceeds) Ordinance (DTPRO) and the Organized and Serious Crime Ordinance (ORSCO), which makes it a criminal offence for a person who knows or has reasonable grounds to believe that any ‘property’ (a definition that is likely to include Bitcoin, Ether and other forms of virtual commodities or virtual assets) in whole or in part represents the proceeds of drug trafficking or crime, to deal with that property. Corporations must also comply with the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO) in relation to terrorism financing. In general, the DTPRO, ORSCO and UNATMO require any suspected transactions involving money laundering, terrorist financing or receipts of crime to be reported to the Joint Financial Intelligence Unit by submitting a suspicious transaction report (STR) as soon as practicable. Failure to file an STR is a criminal offence.

In general, there is no capital gains tax, withholding tax or value added tax (VAT) payable in Hong Kong. That being said, any Hong Kong-sourced income from frequently known cryptocurrencies (e.g., Bitcoin and Ether, which are generally considered virtual commodities in Hong Kong) trading in the ordinary course of business may be treated as income in the case of individual clients, and profits in the case of corporations, and may be subject to income tax and profits tax respectively regardless of whether the trading is done exclusively in cryptocurrency or fiat-to-cryptocurrency exchanges. According to a press release dated 3 April 2019, the Inland Revenue Department of Hong Kong (IRD) states that it does not maintain statistics specifically on tax payable by persons carrying out virtual asset-related activities and that each case should be assessed on the basis of its own individual facts and circumstances. The IRD would also, if necessary, seek relevant information from other tax authorities through the exchange of information mechanism under tax treaties to assess the situation. The IRD has provided further guidance on its treatment of cryptocurrencies in its Departmental Interpretation and Practice Notes dated March 2020. In particular, the IRD makes a distinction between security tokens and utility tokens, as utility tokens would be considered as a prepayment for future goods or services and may be chargeable under profits tax. Furthermore, the IRD clarifies its position that all Hong Kong-sourced profits from cryptocurrency business are chargeable to profits tax, and that broad guiding principles will be applied to determine whether such profits are generated from Hong Kong. In addition, any cryptocurrency that is (1) attained in the process of business transactions; and (2) received as employment income will be taxable, with the value of the cryptocurrency to be determined at the time of accrual.

To the extent where security tokens are concerned, stamp duty is imposed on the transfer of interests in land and certain transfers of stock, and the holder of any token that is linked to such property should be aware of the potential stamp duty payable for the transfer.

Any person who markets and distributes security tokens (whether in Hong Kong or targeting Hong Kong investors) is required to be licensed or registered for Type 1 regulated activity under the SFO.

VI OTHER NEW BUSINESS MODELS

There is no law that regulates self-executed contracts. As long as the execution can comply with the applicable regulatory regime, a self-executed contract would be recognised. For instance, as long as the contract is validly entered into, any automatic transfer of funds or digital assets would be deemed validly made. However, any specific assets that require
registration with local authorities (for example transfer of Hong Kong property or shares in a Hong Kong company) would not be recognised unless the necessary transfer procedure is followed and all necessary filings are made with the government authorities.

Mediation and arbitration are recognised and acceptable methods of alternative dispute resolution in Hong Kong. Under Hong Kong law, parties to a private transaction are at liberty to require any disputes to be resolved through mediation or arbitration instead of court proceedings, provided that the parties clearly record such arrangement in the agreement between them.

It is currently unclear whether a fully automated investment process (i.e., dealing in securities without any human intervention) would be permitted. According to the SFC Online Guideline, robo-advice refers to the provision of financial advice in an online environment using algorithms and other technology tools (which the SFC notes in the SFC Online Guidelines include fully automated investment advice via an online platform with no human intervention) but this does not seem to cover situations where an investment process can be made automatic.

The increasing interest in Hong Kong for blockchain technology has sparked the creation of different business models and even introduced a new industry. One notable business model is the issuance of ‘stablecoins’, which are pegged to the value of a certain currency, for example, the Hong Kong dollar. Such a business model is also influenced by the introduction of the coin to be issued by Facebook, Libra. However, regulators have concerns over the use of stablecoins as they expose the market to significant risks, such as AML issues, banking and financial industry risks, and state-specific treasury policies etc. While there are currently no specific laws in Hong Kong that deal with, prohibit or regulate stablecoins, the PSSVFO is most relevant to the operation and issuance of stablecoins. PSSVFO regulates stored-value facilities that are used for payment for goods and services, whose functions are similar to stablecoins by virtue of storing monetary value and assisting payment using the stored monetary value. Any corporation that wishes to issue a stored-value facility must apply for a SVF licence from the HKMA.

There is also a regulatory requirement on companies that facilitate the issuance of a stored-value facility, which addresses companies that provide the valuable consideration for the issuer.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Codes, programs, source codes or related software are generally protected under the Copyright Ordinance by way of copyright. Copyright arises automatically as long as the work is original and recorded in a material form. Software is usually covered under the category of ‘literary works’ under the Copyright Ordinance. However, mere ideas are not protected and therefore business models may not be protected. There is no regime of registration for copyright in Hong Kong but the Copyright Ordinance grants copyright owners exclusive rights to carry out certain acts in relation to the works, including (but not limited to) distributing the work to the public and copying the work.

Any infringement of an owner’s copyright would give rise to civil liability that the owner can take action on. Depending on the action taken by the infringing party, there may also be criminal liability (for example if the infringing party makes the copyright work for sale or for hire).
In addition to copyright, any invention that is new and involves an inventive step can be patented in Hong Kong via registration as long as it is susceptible of industrial application and does not belong to the excluded classes of inventions through the Patents Ordinance and the Patents (General) Rules. Patents are generally separated into two types, being standard and short-term. Standard patents can last up to 20 years while short-term patents can last up to eight years. However, standard patents are registered based on the registration of a patent granted by one of the designated patent offices – the State Intellectual Property Office in China, the European Patent Office or the United Kingdom Patent Office. Whether a software-related invention used in a fintech business model is capable of being patented will depend on whether the invention is new, involves an inventive step and solves a technical problem, which would be determined on a case-by-case basis. For blockchain corporations, this may be difficult unless they can prove that the software-related invention that relies on blockchain satisfies the requirements set out by the patent office.

It is standard practice for employees or contractors to agree in their employment contracts that all works created by them for the purpose of the employer or client’s business would be considered works created by the employer or client. It is also standard practice for parties to agree that the employee or contractor will sign any documents or do anything necessary to give effect to the transfer of the intellectual property of the works created during the employment.

The PDPO establishes a principle-based regime that regulates the collection, holding, processing and use of personal data of clients in Hong Kong. Businesses in Hong Kong that are ‘data users’ (defined as persons who control the collection, holding and processing or use of personal data) are regulated by the PDPO. The principles which data users must observe mainly relate to notification requirements at the time of collection of personal data, security and access to personal data and accuracy and duration of retention of personal data. There are also particular restrictions regarding the use of client lists to market products.

Under the PDPO, clients do not have a general right to object to processing (including digital profiling) but clients may opt out from direct marketing activities.

VIII YEAR IN REVIEW

i Launch of virtual banks and insurers

In 2019, the HKMA granted a total of eight virtual banking licences to advance its Smart Banking initiative and to promote fintech and innovation in Hong Kong. Certain virtual banks in Hong Kong have already started their trial operation within the HKMA’s Fintech Supervisory Sandbox, and it is currently expected that a number of virtual banks will fully launch operations during 2020, with the first being ZA Bank, which is co-owned by mainland online insurer Zhong An Online P&C Insurance and Sirolink Group, and that virtual banks will be supervised by the HKMA.

The Insurance Authority is also taking steps to encourage greater use of technology by Hong Kong’s insurers. In December 2018, the Insurance Authority granted a virtual life insurer licence to Bowtie Insurance and subsequently in October 2019 granted the first virtual general insurer licence to Avo Insurance, a local insurtech company that offers life, travel and health-related products. These virtual insurers will sell their products online without the use of agents or brokers.
Guidelines for financial services advisory

As mentioned above, the SFC published its Guidelines on Online Distribution and Advisory Platforms in July 2019. The SFC governs the operation of licensed or registered persons (online platforms) when conducting their regulated activities on the online distribution and advisory platforms for investment products.

Regulation of virtual asset trading platforms

The SFC issued a Position Paper in November 2019 to set out a robust regulatory framework for virtual assets trading platforms operating in Hong Kong that provide various trading, clearing or settlement services for virtual assets. It is expected that it will grant the first licence to a virtual asset trading platform in 2020.

IX OUTLOOK AND CONCLUSIONS

The SFC recognised the developments of the fintech market by regulating the virtual asset trading platform. However, it is anticipated that regulators in Hong Kong will remain cautious about virtual assets and will continue to adopt a wait-and-see approach.

The virtual asset trading platform framework is only applicable to platforms where at least one virtual asset or token that is available for trading falls under the definition of a security under the SFO. However, there are still regulatory gaps in the Position Paper that may need to be addressed through further legislative amendments.

The new framework enables the SFC to closely supervise virtual assets trading platforms, which is regarded as one of the fastest developing areas in the recent fintech space. Interactions with the platforms would place the SFC in a better position to design and implement a future regulatory strategy for virtual assets, perhaps including the regulation of virtual assets that do not fall within the current scope of regulation.
Chapter 10

ITALY

Giuseppe Rumi, Federico Vezzani and Tommaso Faelli

I OVERVIEW

Fintech is radically innovating the way financial services are designed and offered and is rapidly transforming the structure of the financial industry. It represents an evolving phenomenon that involves several market segments (e.g., banking activities, payment services, virtual currencies, crowdfunding, peer-to-peer lending and investment services), and heterogeneous tools and techniques (e.g., robo-advice, distributed ledger technologies (DLT) and artificial intelligence (AI)).

The payment services sector appears to be the area that has experienced major developments as, following the Second Payment Services Directive’s (PSD II’s) entry into force and implementation within the Italian legal framework at the beginning of 2018, new business opportunities are offered to fintech companies. In this regard, 2019 witnessed the IPO of Nexi SpA, one of the Europe’s biggest players in the payment services market. Marketplace lending represents another interesting phenomenon in the fintech area, not only for the registered growth rates in terms of volumes in the last few years, but also and especially for the innovative character of the business models deployed. Other developments are also taking place in the credit sector, securities trading and risk management.

Although the benefits of technological changes may take some time to fully materialise, innovation can contribute to reducing costs and information asymmetries, increasing efficiency and competition, and widening access to financial services. Market estimates indicate that investment in financial innovation has increased sixfold at the global level in the last five years. An increase in fintech investments has also been witnessed in the Italian market, although it is still modest compared with other European countries.

In this context, Italian competent authorities appear to be aware that fintech developments could deeply affect the ability of the financial industry to evolve and prosper. At the same time, they are also concerned about the risks that might emerge regarding consumer protection, among other things. Indeed, greater use of digital technologies, which raises the number of potential entry points for cyberattacks, can increase the financial system’s vulnerability and generate institution-specific, financial and operational, and systemic risks.

From a regulatory perspective, despite efforts to arrive at a harmonised approach to fintech regulation, the current legal framework governing fintech is still largely incomplete. Moreover, doubts exist as to how to interpret existing rules, as fintech activities are often difficult to classify based on traditional principles.

1 Giuseppe Rumi, Federico Vezzani and Tommaso Faelli are partners at BonelliErede.
The Italian government and competent authorities are thus developing an increasingly fintech-friendly environment. For instance, the Bank of Italy (BoI) has long been in contact with market operators offering innovative solutions: since 2017 it has had an innovation hub, ‘FinTech Channel’, on its website through which the BoI directly interfaces with operators in a digital environment to assess their compliance with legislation, identify potential problems and consider changes to the rules and procedures applied at national level.

Moreover, to ensure adequate protection of consumers, investors and the financial market in general, and to stimulate competition in the market, in 2019 the Ministry of Economy and Finance (MEF) was granted the power to adopt one or more regulations to set the conditions and methods for conducting trials concerning fintech activities aimed at pursuing service and product innovation in the financial, credit, insurance and regulated market sectors through new technologies (known as sandboxes). Simultaneously, a new fintech committee was established within the MEF to define the objectives and programmes and implement the actions necessary to foster fintech’s development in Italy.

The BoI and the Italian Companies and Stock Exchange Commission (Consob) recently issued several regulations implementing the provisions introduced by the Italian government on blockchain, cryptocurrencies and crowdfunding, among other things (see Sections IV and V). Consob has also launched several initiatives, including a public consultation on crypto activities and initial coin offerings (ICOs) adopting blockchain technologies, as well as research programmes concerning robo-advice, blockchain, marketplace lending, and other fintech-related topics. The initiatives are aimed at understanding more about the aspects that can influence the financial system and at regulating the fintech phenomenon.2

Finally, with regard to tax incentives, fintech companies can benefit from, among other things:

a an innovative start-up regime, according to which – direct or indirect – investments in innovative start-up companies are partially deductible (if certain conditions are met);

b a patent box regime that provides for a 50 per cent exemption from corporate tax in relation to those incomes arising from direct use or licensing of qualified intangible assets (e.g. patents, know-how); and

c tax credit on research and development activities, according to which companies can benefit from a tax credit ranging from 6 per cent to 12 per cent (depending on the kind of expenses) of the R&D expenses (with a maximum cap).

II REGULATION

i Licensing and marketing

Currently, no specific fintech licence or regulatory framework exists for fintech sector activities. The only exception is the management of crowdfunding portals, which is regulated by Article 50 quinquies of Legislative Decree No. 58 of 24 February 1998 (the Italian Financial Act) and Consob Regulation No. 18592 of 26 June 2013, which requires an authorisation for portal managers other than banks and investment firms (see Section IV).

As a general rule, specific authorisation is always required for activities that qualify as reserved activities under Italian law, regardless of the (technological) means used to carry

---

2 See, for example, the series of contributions and documents dedicated to fintech launched by Consob, in collaboration with the main Italian universities, in March 2018.
out them. Therefore, fintech firms that perform banking activities, investment services and asset management activities (including robo-advice and digital asset and wealth management services), payment services or insurance activities are subject to the general Italian and European regulatory framework; thus, they must have obtained authorisation from the competent supervisory authorities (the BoI, European Central Bank, Consob and the Italian Insurance Supervisory Authority (IVASS)) and comply with the relevant legal framework (including prudential and governance requirements and business conduct rules).

Considering the absence of a clear and all-encompassing Italian regulatory framework applicable to fintech activities, the marketing of fintech products and services provided by regulated fintech entities is currently governed by the same rules applicable to any other regulated entity (e.g., Italian consumer protection law and BoI regulations on the transparency of banking and financial transactions and services).

With regard to credit information services, the Italian framework sets out different rules depending on the private or public nature of the credit information system. Notably, private information systems contain information on credits provided by participating companies, but registration is not mandatory for banks or financial intermediaries. Conversely, these intermediaries are required to enrol with the Central Credit Register,3 an information system regarding customers’ risk position managed by the BoI, that is intended to, among other things, improve the quality of credit provided by intermediaries. The Central Credit Register can be accessed only by registered intermediaries and, on request, by individuals or entities. The register contains information on credit amounting to €30,000 or more.

ii Cross-border issues

In Italy, regulated activities can be carried out either through the establishment of a branch or under the regime of the freedom to provide services. As outlined in Section II.i, Italy has no ad hoc regulatory framework in place – or passporting procedure – that specifically governs the provision of fintech products and services. Therefore, if a fintech company intends to offer products or services in Italy that – regardless of the technology used – fall within the definition of a reserved activity, the company will need to comply with all the relevant regulations. More specifically, EU-licensed companies, regardless of their fintech nature, benefit from the passporting procedure set out by the main EU directives governing the provision of regulated activities (e.g., the Fourth Capital Requirements Directive,4 the Second Markets in Financial Instruments Directive (MiFID II), Solvency II, the Undertakings for Collective Investment in Transferable Securities Directive, the Alternative Investment Fund Managers Directive or PSD II). These passporting procedures require, among other things, a simple notification to the competent authorities of the home and host Member States, without, in principle, the need to obtain a local licence in the host Member State.

If non-EU companies wish to provide fintech products or services that fall within the definition of a reserved activity in Italy, they will need to obtain prior authorisation from the relevant Italian competent authority (the BoI, Consob or IVASS, depending on the type of activity).

3 The rules on BoI’s Central Credit Register are set out in BoI Circular No. 139 of 11 February 1991, as subsequently amended and supplemented.

4 As recently amended by Directive (UE) 2019/878.
Furthermore, companies wishing to actively market services and products in Italy might be required to obtain prior authorisation and meet specific requirements depending on, among other things, the type of services and products, the level of information provided on such services and products and whether the marketing activity is targeted at Italian residents.

In Italy, foreign exchange and currency controls are not subject to restrictions except for those concerning banknote circulation. Additionally, as a general rule, the Italian legal framework does not limit foreigners’ rights to own Italian companies. However, if a foreigner wishes to acquire a significant holding in a supervised entity (e.g., bank, financial intermediary, investment firm or asset management company), specific rules set out in the Italian Banking Act and in the Italian Financial Act apply. These rules require the potential acquirer to, among other things, file a prior authorisation application with the relevant competent authority and meet specific integrity, fairness, transparency and professionalism requirements.

Law No. 58 of 28 June 2019 granted Consob the power to order internet connectivity providers to deny access from Italy to foreign websites through which unauthorised financial services are offered. Since July 2019, more than 160 websites have been blocked to prevent licence abuse and guarantee adequate protection for retail investors.

III DIGITAL IDENTITY AND ONBOARDING

The Italian government has been implementing a digital identity public system (SPID) through the Agency for Digital Italy (AGID) since 2016. SPID allows citizens (including those resident in other countries) to access (through personal login credentials) online services provided by public and private entities.

Personal login credentials for SPID are provided by private identity providers licensed by the AGID. Citizens are therefore free to decide which entity to entrust their digital identity. SPIDs can be implemented inside a business under a specific agreement with the AGID and an agreement with identity providers. Examples of both agreements are available on the government’s website. Payment terms and conditions are set out in the agreement with the AGID and cannot be amended by the parties. Few private parties are currently implementing SPIDs because of the high cost of doing so.

Furthermore, banking and investment services providers can implement fully digitalised onboarding of clients, provided that additional requirements to the physical onboarding are met. These requirements, which are generally set out for the provision of banking and investment services through long-distance communication, mainly concern transparency (e.g., sending pre-contractual and contractual documents through a durable medium), anti-money laundering (AML) identification duties (e.g., double checking of identification data) and consumer’s protection (e.g., client’s right withdraw within 14 days from entering into the contract).

---

5 e.g., the cross-border transport limits on physical currency and its equivalents (no more than €10,000) and limits on cash payments (no more than €3,000).
6 See, for example, Article 25 of the Italian Banking Act and its implementing regulations.
7 Data as of 1 March 2020. Source: Consob website.
8 See: (1) BoI’s transparency provisions of 29 July 2009, as subsequently amended, for banking and payment services; and (2) Consob’s Intermediaries Regulation No. 20307 of 15 February 2018, for investment services.
9 See the BoI’s regulation of 30 July 2019 on customer due diligence.
10 See Legislative Decree No. 206 of 6 September 2005 (Italian Consumers Code).
An innovative remote video-identification procedure to meet customer due diligence requirements for AML purposes is now regulated by the BoI’s regulation of 30 July 2019.11

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i Crowdfunding

A high-level definition of crowdfunding was recently introduced by Law Decree No. 34 of 30 April 2019 (converted into Law No. 58 of 28 June 2019): crowdfunding is the instrument through which a number of investors directly finance households and enterprises by means of online platforms.12

Nevertheless, Italy was one of the first countries in Europe to introduce specific legislation governing equity crowdfunding, which is laid down in the Italian Financial Act13 and Consob Regulation No. 18592 of 26 June 2013 (Crowdfunding Regulation).14 Under this legislation, the management of equity crowdfunding portals is limited to:

a investment firms and banks authorised to provide investment services, which are considered ‘de facto managers’ and require no specific licence; and

b portal managers other than those under point (a), which need to be duly authorised and enrolled on a special register managed by Consob.15

Moreover, equity crowdfunding portals may only be used to offer to the public financial instruments that are issued by small and medium enterprises (SMEs), innovative start-ups, collective investment schemes, social enterprises and companies that mainly invest in SMEs.

In this respect, Law No. 145/2018 (the 2019 Budget Law) amended the Italian Financial Act by introducing the ability to offer also debt instruments through crowdfunding portals, provided that this is carried out through a separate area of the portals and that these instruments are addressed only to professional investors and other categories of investors identified by Consob. With Resolution No. 21110 of 10 October 2019, Consob amended the Crowdfunding Regulation to align the secondary regulations with the new provisions in the Italian Financial Act. The Crowdfunding Regulation was further amended in 2020, through Consob Resolution No. 21259 of 6 February 2020, which (among other things) removed the obligation for portal managers to participate in an investor-compensation scheme but maintained the obligation to take out insurance to cover professional liability.

ii Debt financing and lending platforms

One main area in which Italian fintech companies are growing is debt financing, which includes lending activities and secondary market trading using online platforms.

More specifically, peer-to-peer lending and social lending have experienced rapid growth in recent years and represent one of the more mature fintech sub-sectors, even though

11 See Annex 3 to the BoI’s regulation on customer due diligence published in July 2019 after a public consultation started in April 2018.
12 See Article 18, Paragraph 4, of Law Decree No. 34/2019.
13 As amended by Law Decree No. 179/2012, converted into Law No. 221/2012.
14 http://www.consob.it/documents/46180/46181/reg_consob_2013_18592.pdf/54eae6e4-ca37-4c59-984c-cb54d90a8393. Consob also has the following web page with all the relevant crowdfunding information: www.consob.it/web/investor-education/crowdfunding#c2.
15 Currently, there are 37 portal managers enrolled on the register managed by Consob.
no specific regulation governs them so far. At the end of 2016, the BoI clarified that peer-to-peer lending and social lending may fall under the definition of the following activities, which are reserved to duly authorised entities: lending, collection of savings and payment services.\textsuperscript{16}

Additionally, the BoI defines lending-based crowdfunding as an activity carried out through an online platform that allows several parties to collect repayable funds and clarifies, among other things, that the following activities do not constitute ‘collection of savings’:

\begin{enumerate}
  \item managers of online platforms: if they receive funds to be held in payment accounts that can be used only to provide payment services by entities authorised to carry out payment services or to issue electronic money; and
  \item borrowers: if they acquire funds from:
    \begin{enumerate}
      \item individual lenders (following personalised negotiations) that are supported by the platform manager only to enable the execution of the agreement; or
      \item entities subject to prudential supervision.
    \end{enumerate}
\end{enumerate}

Law Decree No. 34/2019 (converted into Law No. 58/2019) introduced a high-level definition of social lending: the instrument through which a number of parties may request, through online platforms, repayable funds for personal use or financing for a project to a number of potential lenders (including institutional investors).\textsuperscript{17}

Invoice lending and invoice trading are other businesses that an increasing number of online platforms are breaking into. Fintech firms involved in these activities adopt business models that normally require prior authorisation to operate as banks or financial intermediaries. However, limited cases exist of non-regulated fintech firms managing online platforms without entering into any lending agreements with the final customers.

With regard to trading loans on a secondary market, purchasing receivables qualifies as a lending activity that may be performed only by banks, financial intermediaries enrolled on the BoI’s register under Article 106 of the Italian Banking Act, and alternative investment funds that invest in receivables.\textsuperscript{18} Furthermore, as to securitisations, special purpose vehicles may purchase receivables under a simplified procedure that reduces transfer costs. This also ensures that all charges and guarantees retain their validity and priority, without the need for any additional formality, provided that all notification duties are complied with.\textsuperscript{19}

iii Payment services

Innovative payment services represent one of the most prominent and widespread fintech developments in Italy. The provision of payment services in Italy is subject to the BoI’s prior authorisation under Article 114 novies of the Italian Banking Act.

Following PSD II’s implementation in Italy with Legislative Decree No. 218/2017, the Italian Banking Act now includes two new payment services: payment initiation and account information services. In July 2019, the BoI amended its regulation on payment service providers to introduce rules on third-party providers (TPPs), which are typically payment initiation service providers (PISPs) and account information service providers (AISPs).\textsuperscript{20}

\textsuperscript{17} See Article 18, Paragraph 4, of Law Decree No. 34/2019.
\textsuperscript{18} See Article 106 of the Italian Banking Act.
\textsuperscript{19} See Article 4, Paragraph 1, of Law No. 130 of 30 April 1999 and Article 58 of the Italian Banking Act.
\textsuperscript{20} See the BoI regulation on payment institutions and electronic money institutions of 23 July 2019.
PISPs and AISP's are fintech companies that must be duly authorised and comply with the regulatory framework on payment services; and must offer payment initiation and account information services by exploiting the new business opportunities provided by technological innovation. These new services require access to data and accounts held by credit institutions or other payment services providers. Therefore, each payment service provider with payment accounts accessible online (mainly banks) is now required to provide access – through at least one access interface – to their clients' data and accounts to other TPPs to enable them to carry out their business effectively. In line with the EBA's opinion of 16 October 2019, the BoI recently pointed out that the deadline for the migration to authentication approaches that comply with the EU framework on strong customer authentication has been postponed to December 2020.

iv  Collective investment schemes

Collective investment schemes are mainly regulated in Italy under the Italian Financial Act and its implementing regulations, which do not envisage any ad hoc provisions applicable to fintech entities falling under the definition of managers of collective investment schemes. Therefore, these fintech entities must comply with the general legal framework on asset management activities under the Italian Financial Act.

V  CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

In February 2019, Law No. 12/2019 introduced the definition of distributed ledger technology (DLT) to recognise the legal effects of electronic time stamps under Article 41 of EU Regulation No. 910/2014 and the storage of an electronic document through a DLT. Moreover, in May 2019 the AGID established a working group tasked with preparing the implementing technical standards providing the DLT requirements that ensure these transactions have legal effect, which are yet to be published.

These new provisions mark a significant step forward in developing blockchain technology in Italy and follow Italy's subscription to the European Blockchain Partnership Initiative in September 2018 and the signing of the Southern European Countries Ministerial Declaration on Distributed Ledger Technologies in December 2018.

With regard to virtual currencies, the first relevant and binding definition of virtual currency was introduced by Legislative Decree No. 90/2017, which implemented Anti-Money
Laundering Directive (AMLD) IV and amended Italian AML law (Legislative Decree No. 231/2007 – the AML Decree). The AML Decree was subsequently further amended by Legislative Decree No. 125/2019, which implemented AMLD V in Italy.

Virtual currency is now defined as:

> the digital representation of value, not issued nor guaranteed by a central bank or a public authority and not necessarily linked to a value having a legal tender, that is used as a means of exchange for the purchase of goods and services or for investment purposes and that is transferred, stored and traded through electronic devices.\(^{27}\)

The AML Decree also provides ad hoc definitions of virtual currency service providers and digital portfolio service providers. A virtual currency service provider is:

> any natural or legal person who provides to third parties, in a professional manner, also online, useful services to the use, exchange, storage of virtual currency and to their conversion from or into legal tender currencies or into value digital representations, including digital representations convertible into other virtual currencies as well as issue, offer, transfer and compensation services and any other functional service to the acquisition, negotiation or brokerage in the exchange of the same currencies.\(^{28}\)

Moreover, a digital portfolio service provider is:

> any natural or legal person who provides to third parties, in a professional manner, also online, private cryptographic key safeguarding services on behalf of their clients, in order to hold, store and transfer virtual currencies.\(^{29}\)

Under the AML Decree, these providers are subject to specific notification and enrolment requirements, which will be set out in a decree from the MEF (currently available only in its draft version).\(^{30}\) Once this Decree enters into force, virtual currency service providers will be required to:

- notify the MEF of the commencement of their activities; and
- enrol with a special section of the currency exchangers’ register.

Failure to comply with the notification duty under point (a) may result in the application of specific administrative penalties.

Additionally, the AML Decree, as amended by Legislative Decree No. 125/2019, extends AML compliance obligations (i.e., customer due diligence, storage of data, notification of suspicious transactions and abstention in case of impossibility to carry out the customer due diligence) to providers engaged in services related to the use of virtual currency

---

\(^{27}\) See Article 1, Paragraph 2, let. qq) of Legislative Decree No. 231 of 21 November 2007, as amended by Legislative Decrees No. 90 of 25 May 2017 and No. 125 of 4 October 2019.

\(^{28}\) See Article 1, Paragraph 2, let. ff) of the AML Decree.

\(^{29}\) See Article 1, Paragraph 2, let. ff bis) of the AML Decree.

\(^{30}\) In January 2018, the MEF published a decree for consultation setting out the timing and conditions for the notification of the commencement of virtual currency activities by service providers. However, the final version of this decree has yet to be published.
and to digital portfolio service providers.\textsuperscript{31} This extension – and in general the application of AML duties to parties operating in the cryptocurrencies and tokens field – has raised concerns, at both European and national level, owing to the volatility of virtual currencies.\textsuperscript{32} The above definition of virtual currencies first appeared in a communication published by the BoI in 2015,\textsuperscript{33} which contained clarifications of the characteristics of virtual currencies; and, in line with the European Banking Authority (EBA),\textsuperscript{34} a warning about the use of these currencies, as they could result in a breach of Italian regulations with the risk of criminal penalties.\textsuperscript{35}

In 2018, the BoI issued another communication declaring its adherence to the European Supervisory Authorities (ESAs) warning on virtual currencies\textsuperscript{36} and discouraging Italian banks, other supervised entities, and consumers from buying or selling virtual currencies following several scandals involving cryptocurrencies.\textsuperscript{37} The BoI also highlighted that several non-regulated entities are involved in trading virtual currencies and, as they are not subject to AML regulations, their activity could pose risks. Moreover, Consob published a consumer warning regarding the cryptocurrencies-related risks.\textsuperscript{38} Additionally, in 2018 Consob adopted several measures regarding companies that offer investments in cryptocurrencies and initial coin offerings (ICOs), qualifying their activity as public offering of financial products (i.e., financial instruments and any other form of financial investment)\textsuperscript{39} without the necessary prior authorisation.\textsuperscript{40} Furthermore, in March 2019, Consob published a discussion paper

\textsuperscript{31} See Article 3, Paragraph 5, let. i) and let. i \textit{bis}) of the AML Decree.

\textsuperscript{32} Indeed, the volatility of virtual currencies and the difficulties in identifying the virtual wallet’s owner appear inconsistent with AML duties (see, for example, Question No. 3-2018/B of the Italian National Council Notaries).

\textsuperscript{33} See Bank of Italy, 30 January 2015: www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf.

\textsuperscript{34} See EBA warning on the use of virtual currencies at the following link: https://eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf.

\textsuperscript{35} See Articles 130 (abusive activity of collection of savings), 131 (abusive banking activity) and 131 \textit{ter} (abusive provision of payment services) of the Italian Banking Act, and Article 166 (abusive provision of investment services) of the Italian Financial Act.


\textsuperscript{37} i.e., the bankruptcy of the well-known Japanese exchange facility MtGox and, more recently, in January 2019, the bankruptcy of the Italian company BG Services S.r.l., which managed the BitGrail exchange in Nano cryptocurrency.

\textsuperscript{38} http://www.consob.it/documents/46180/46181/rischi_criptovalute.pdf/51942a52-4815-4a55-97f9-0bd95e5061d1.

\textsuperscript{39} In several resolutions and communications Consob clarified that ‘any other form of financial investment’ refers to investments that include: (1) the use of capital; (2) an expectation of return; and (3) the related risk. See, among other things, Consob Communication No. DEM/3082035 of 19 December 2003 and Consob Resolution No. 14422 of 13 February 2004.

\textsuperscript{40} See, for example, Consob Resolutions No. 20693 of 14 November 2018, No. 20741 of 12 December 2018 and No. 21148 of 13 November 2019, whereby Consob suspended an offer of tokens and an offer of virtual currencies under Article 99 of the Italian Financial Act.
for consultation at national level on the possibility of regulating cryptoassets and ICOs. The discussion paper resulted in the publication of a final report in January 2020 that addresses the main issues raised by recipients.\footnote{http://www.consob.it/documents/46180/46181/ICOs_rapp_fin_20200102.pdf/70466207-edb2-4b0f-ac35-dd8449a4baf1.}

As of today, there are no specific tax provisions governing cryptocurrencies in Italy. However, the Italian tax authority has recently issued some resolutions providing preliminary guidelines on the tax treatment of cryptocurrencies.

According to the Italian tax authority, any gains deriving from the disposal or the conversion of cryptocurrency shall be treated as foreign currencies and therefore:

\begin{itemize}
\item[a] individuals shall be taxed – at 26 per cent tax rate – if, during the fiscal year and for at least seven consecutive days, the threshold of ownership of cryptocurrency exceeds €51,645.69; and
\item[b] companies are subject to tax under the general corporation tax regime for profits and losses (currently, corporate income tax rate is 24 per cent).
\end{itemize}

With reference to VAT, the Italian tax authority is aligned with the position of the European Court of Justice – the \textit{Skatteverket} case (C-264/14) – according to which, cryptocurrency trading is a commercial activity that falls within the scope of VAT but shall be considered as exempt from VAT by virtue of Article 135(1)e of the VAT Directive, which deals with currency-related transactions.

The Italian tax authority has also provided some guidelines with reference to the ‘utility token’ (those that enable the token’s holder future access to the products or services offered by the token’s issuer or a third party). These financial instruments are assimilated to ‘vouchers’ from the token’s issuer perspective and, as such, are taxed when the goods (or services) are transferred to the token’s holder. Any gains deriving from the disposal of utility token are subject to tax in the hand of the holder; the latter could be either an individual or a company. In the first case, the relevant gains are subject to 26 per cent tax rate, otherwise they are subject to corporate taxation at a 24 per cent tax rate.

\section*{VI OTHER NEW BUSINESS MODELS}

Law No. 12/2019 also introduced the definition of smart contracts as part of DLT. Indeed, smart contracts are defined as ‘a computer program that works through distributed ledger technology and whose performance automatically binds two or more parties based on effects defined by the parties themselves’.

Smart contracts on a DLT are considered entered into in writing if the AGID’s guidelines are complied with. However, the AGID has yet to issue any such guidelines. Moreover, to ensure that smart contracts are concluded in writing, an electronic signature system that is able to identify the parties must be in place. The system must be an advanced electronic signature or a qualified one; both are envisaged by European Regulation No. 1999/93 and Italian Legislative Decree No. 82/2005.

Thus, smart contracts are currently specifically defined as operating only through a DLT, but this does not mean that their use is prohibited elsewhere. Indeed, smart contracts are generally defined as:
Unless specifically prohibited, smart contracts can be used provided they meet the certainty requirements set out by law.

In general, fintech encompasses a wide range of financial services and products that intersect with technology. Banks and other traditional players are gradually evolving their business models by increasing the level of their services. Innovations related to, among other things, mobile and digital payments, cloud computing, data governance and risk management software have increased the efficiency of banking activities and allow cost reductions regarding the material provision of some services. Indeed, banks are reducing their territorial presence in favour of more digitalised business models. Although the effects of digitalisation in an economy based on territorial rooting are yet to be proven, several banks have started to develop full-service banking businesses almost exclusively based on digitalised platforms. Furthermore, to accelerate this process, many banks are collaborating with existing fintech companies (through partnerships or acquisitions of a stake in these companies) to immediately acquire the know-how needed to implement digitalised business models.

At the same time, fintech companies frequently need to rely on banks or other supervised entities to implement business models – such as digital payments or financing platforms – that require authorisation from the competent supervisory authorities. In this respect, the main regulatory issue raised by new digitalised services performed by fintech companies concerns identifying those businesses that could fall within the scope of reserved activities, particularly if these businesses are operated without reliance on supervised entities.

The range of fintech products and services also covers the use of artificial intelligence to support the entire investing process (e.g., robo-advice and algorithmic trading). In this respect, although robo-advice is not expressly regulated under the Italian legal framework, from a regulatory standpoint, it could fall within the definition of investment advice (see Section II.i). On this basis, it could therefore be considered a reserved activity that only duly authorised subjects are permitted to carry out and that must comply with the Italian regulatory framework on investments services. As to algorithmic trading, under the Italian Financial...

---


43 See, for example, Buddybank (the digital bank powered by Unicredit), CheBanca (part of Mediobanca’s group) and Widiba (part of MPS group).

44 See, for example, the partnership between UBI Banca (the fourth largest Italian bank) and Fabrick, a fintech company specialised in open banking services and the acquisition by DEPObank of a controlling stake in PrestaCap, a digital lending platform.

45 See Consob Regulation No. 20307 of 15 February 2019.
Italy

Act\textsuperscript{46} and Consob Regulation No. 20249 of 28 December 2017, banks and investment firms can engage in algorithmic trading or high-frequency algorithmic trading, thus operating with minimal or no human intervention, subject to notification and recording duties to Consob.

Consob recently published its Strategic Plan for 2019–2021,\textsuperscript{47} which includes several initiatives to assess the impact of digitisation on financial intermediation processes (including robo-advice) with the aim of promoting innovation while ensuring investor protection. Moreover, to promote and support entrepreneurship, stimulate market competition and ensure adequate protection of consumers, investors and the capital market, the MEF was recently granted the power to adopt one or more regulations to define the conditions and methods for conducting trials concerning fintech activities (known as regulatory sandboxes).\textsuperscript{48} Simultaneously, a new fintech committee was established within the MEF to implement the actions necessary to foster fintech’s development in Italy.\textsuperscript{49}

Cyberattacks are one of the main emerging risks associated with the use of technology in financial services. To address this issue, Legislative Decree No. 65 of 18 May 2018 implemented Directive (EU) 2016/1148 concerning measures for a high common level of security for network and information systems across the European Union. In addition, the BoI and Consob recently agreed to adopt a common cyber-resilience strategy for Italy’s financial market infrastructure to improve financial security and business continuity.\textsuperscript{50} In line with this, in 2016 the BoI and the Italian Banking Association (ABI) sponsored the establishment of the Italian Financial Cybersecurity unit,\textsuperscript{51} which coordinates information sharing and cyber-threat intelligence among participating financial companies, allowing them to share critical information and enhance the awareness of cyber risk beyond what would have otherwise been possible within the confines of their own organisations.\textsuperscript{52}

As to websites comparing financial products offered or providing information about the financial products themselves, there are no specific privacy provisions or competitive rules, but these legislative provisions can be relevant. In addition, websites covering the insurance sector feature tight regulation that requires comparison websites to be authorised by IVASS,\textsuperscript{53} as also provided by the Insurance Distribution Directive.\textsuperscript{54} Conversely, banking and financial fields do not include any ad hoc regulation for third-party product-comparison, if no banking or financial products marketing is carried out.

\textsuperscript{46} See Article 67 \textit{ter} of the Italian Financial Act.
\textsuperscript{47} http://www.consob.it/documents/46180/46181/ps1921.pdf/3a2f91c1-7541-4c2c-b281-a21854f4e159.
\textsuperscript{48} See Article 36, Paragraph 2 \textit{bis}, of Law Decree No. 34/2019.
\textsuperscript{49} See Article 36, Paragraph 2 \textit{octies}, of Law Decree No. 34/2019.
\textsuperscript{50} See the BoI’s press release of 16 January 2020: https://www.bancaditalia.it/media/comunicati/documenti/2020-01/cs_BIConsob_20200116_ENG.pdf?language_id=1.
\textsuperscript{51} https://www.certfin.it/.
\textsuperscript{52} Recently, Consob also adhered to the Italian Financial Cybersecurity unit. See the press release of 3 December 2019: http://www.consob.it/documents/46180/46181/cs_20191203_en.pdf/3f1413fo-d313-4c66-85c3-b1386c8e60ea.
\textsuperscript{53} See Articles 106 and 108 of Legislative Decree No. 209 of 7 September 2005.
\textsuperscript{54} See Article 2, Paragraph 1, No. 1 of Directive 2016/97/EU.
VII INTELLECTUAL PROPERTY AND DATA PROTECTION

It is essential for fintech businesses to generate the most possible value from the innovative and technological tools and systems they use. Therefore, protecting these tools and systems with intellectual property rights when possible is extremely important.

Software patentability is generally excluded because software cannot be considered an invention per se (Article 45 of the Italian Industrial Property Code). Although software is sometimes patent eligible, patents are excluded in most cases in the fintech field. However, Italian law envisages software safeguards through copyright protection (Article 64 bis of the Italian Copyright Law), which is granted if the software meets the creative requirements set out in the copyright law.

Fintech businesses are increasingly using open-source software or standard software as a base on which to develop customised solutions for their businesses. In these cases, attention must be paid to the presence of copyleft clauses that often impose to disclose the source code of the developments made. According to the applicable terms, obligations to disclose may vary.

Furthermore, business knowledge can be protected as a business secret. This protection ensures that no-one can use secret information developed for business purposes. The fact that the information is secret ensures protection is granted.

Specific rules must be set out in agreements between parties to ensure that the owner of the IP rights over any invention or software created under a contractual relationship is clear.

The following rules apply to employment relationships:

a inventions by the employee in performing his or her work duties: the employer is the owner of IP rights over the employee’s inventions;

b inventions by the employee in performing his or her work duties, even if invention is not a specific work duty: the employer is the owner of IP rights over the employee’s inventions, but the employee has the right to be fairly remunerated for the invention; and

c inventions by the employee outside his or her work duties, but connected with the employer’s field of business: the employee is the owner of IP rights over the inventions, but the employer has a pre-emptive right over the inventions.

In the fintech field, it is necessary to ensure that personal data is lawfully processed in compliance with European Regulation 2016/679 (General Data Protection Legislation – GDPR, which came into force on 25 May 2018) and Italian legislation (specifically Legislative Decree No. 196/2003, the Privacy Code, recently amended by Legislative Decree No. 101/2018). Indeed, sensitive information relating to the financial assessment of natural persons are frequently processed, and a large amount of correct information is gathered to ensure the legal obligations imposed on financial intermediaries are met. The legal obligations deriving from MiFID II and from AML legislation are a prime example. Both require that information be gathered to profile clients and conduct risk analysis to provide the most profitable investment portfolio for both financial intermediaries and clients. Although profiling is mandatory by law, the GDPR must be complied with, particularly information and transparency duties that require disclosure of the rules governing the profiling system if requested by the data subject or client. This is a very sensitive area because complying with the data subject’s right could contrast with the legal entity’s right to protect business information and keep it secret.
Big Data plays a strategic role in the fintech field and, to ensure business growth, fintech businesses need to have access to advanced technology and well-structured databases. Credit and commercial information systems also play a strategic role in this sector by providing information and thus meeting fintech operators’ business needs. The activities performed by these systems are regulated by law and, within the privacy legislation, by specific codes of conduct. It must be underlined that large differences exist between the two information systems. As outlined in Section II.i, credit information systems can be public (i.e., the Central Credit Register managed by the BoI) or private, and only financial intermediaries (and other entities under the BoI’s control) may supplement the databases and ask for information to be extracted from the databases. Conversely, commercial information systems provide information collected from public sources and are available to the public. Commercial information systems are thus clearly fundamental for payment institutions and, especially since PSD II’s entry into force, their importance in the fintech field continues to increase. In 2019, the Italian Data Protection Authority issued specific codes of conduct for the processing of commercial and credit information providing, inter alia, for strict regulation of credit-score databases, modalities and time limits for the collection and preservation of log files regarding banking transactions.

VIII YEAR IN REVIEW

As the results of a recent survey launched by the BoI and published in December 2019 show, financial sector players’ interest in fintech continues to grow. The BoI report highlights, among other things, that the Italian financial system has planned investments in fintech projects for a total of approximately €390 million for 2019–2020. These include collaborations with existing fintech companies (in the form of partnerships or acquisition of a stake in these companies), technologies that improve the efficiency of internal controls systems, open banking and payment services, technologies that facilitate the conclusion of cross-border transactions, robo-advisers, crowdfunding, cloud computing, cybersecurity, AI, DLT and smart contracts.

Traditional financial institutions such as banks or insurers no longer regard fintech companies as competitors, but rather increasingly view them as potential partners in developing and improving new or existing business models. In fact, traditional financial operators are responding with the following strategies to adapt their current market demands:

a development of platform services;

b acquisitions of, or partnerships with, fintech companies; and

c creation of pure digital banks.

A significant number of projects have been launched or are about to be launched in Italy. Non-banking intermediaries have focused their attention on the same needs, demands and issues that banks are concerned with. However, their involvement in investment projects

55 https://www.bancaditalia.it/media/notizia/indagine-fintech-nel-sistema-finanziario-italiano/.
is still limited from a quantitative standpoint, with the focus currently being mainly on payment services, new forms of financial intermediation, high-frequency trading, robo-advice and crowdfunding.

Against this backstop, the Italian regulatory framework has undergone significant reforms that have impacted the fintech sector. More specifically, throughout 2019 and 2020, the following regulations (among others) were issued or placed under consultation to comply with the EU framework and establish a fintech-friendly environment:

a. the amended version of the BoI’s supervisory instruction to payment institutions was published in July 2019 to implement PSD II (see Section IV.iii);

b. Consob Regulation No. 18592 of 26 June 2013 on crowdfunding was amended and supplemented in October 2019 and February 2020 to implement the new provisions introduced by the 2019 Budget Law and by Legislative Decree No. 165/2019, which amended the Italian Financial Act (see Section IV.i);

c. Law No. 12/2019 introduced the definitions of DLT and smart contracts (see Section V);

d. the BoI’s provisions on customer due diligence duties for AML purposes were published in July 2019 (see Sections III and V);

e. Legislative Decree No. 125/2019 amended the AML Decree by introducing the definition of digital portfolio service providers and modifying the definitions of virtual currencies and virtual currency service providers (see Section V);

f. Law Decree No. 34/2019, converted into Law No. 58/2019:
   • introduced a regulatory sandbox in Italy and established the fintech committee within the MEF (see Section VI); and
   • provides high-level definitions of crowdfunding and social lending (see Sections IV.i and Section IV.ii);

g. a public consultation launched by Consob on ICOs and crypto activities took place between May 2019 and January 2020 (see Section V); and

h. a public consultation launched by the MEF in February 2020 on a draft decree providing the implementing provisions of the regulatory sandbox and the fintech committee introduced by Law No. 58/2019 (see Section VI).

At the European level, following the 2018 action plan on how to harness the opportunities created by technology-enabled innovation in financial services, in December 2019 the European Commission placed two proposals under consultation, one concerning the establishment of an EU framework for markets in cryptoassets and the other a digital operational resilience framework for financial services. Moreover, in December 2019, the expert group on regulatory obstacles to financial innovation delivered its final report to the European Commission, which outlines 30 recommendations on regulation, innovation and finance.

---

56 For example, the BoI survey of December 2019 highlighted that the investments in fintech made by Italian asset management companies and Italian investment firms represent less than 1 per cent of the overall amount of investments made by financial sector’s incumbents.


Finally, the EBA published several reports throughout 2019 and some in 2020 on, for example, cryptoassets, regulatory sandboxes and hubs, the impact of fintech on payment institutions and e-money institutions’ business models, the authorisation approaches in relation to fintech activities, and the development, implementation and adoption of Big Data and advanced analytics.60

IX OUTLOOK AND CONCLUSIONS

Technology-enabled innovation in financial services is fast developing and offers numerous advantages. Indeed, fintech opened financial intermediation and credit markets to new players, which is bound to change the way traditional intermediaries operate. Moreover, fintech has the potential to, among other things:

a increase efficiency and reduce costs;

b improve access to, and provision of, financial services;

c enhance the customer experience; and

d create markets for new and innovative financial services and products.

As technology continues to break down the barriers to entry in the bank and financial services markets, banks and other regulated entities are reacting to this changing environment and adopting online banking offerings. This involves them shifting the distribution of their standard services to online platforms via multichannel networks, thereby reducing the number of physical branches, which allows the remaining branches to specialise in high value-added services (e.g., private banking, corporate finance and advisory).

Technology is being leveraged to improve the efficiency of middle- and back-office processes, and to provide more effective risk management tools. Fintech technologies and products offer a wide range of possibilities, and can be instrumental in improving the quality of services offered to clients and give market players an important competitive edge. They can also present further opportunities to fully exploit the advantages of an integrated European financial services market, since they facilitate the distribution of retail products and services on a cross-border basis.

Fintech may also mean that old risks take new forms and that new (substantially increased) risks, such as cyber-risks, arise. As mentioned in Section VI, the BoI and Consob recently agreed to adopt a common cyber-resilience strategy for Italy’s financial market infrastructure to improve the financial security and business continuity.

A wide variety of fintech businesses are currently operating in Italy in almost every sub-sector of the fintech industry. According to the most recent information, almost 300 fintech companies are based in Italy, and this number continues to grow. Crowdfunding is the largest sub-sector of the fintech industry, followed by payment services, asset management, blockchain, virtual currencies, insurance and peer-to-peer lending. A wide range of innovative fintech solutions have recently been developed in the Italian payment services sector, mainly through apps that provide alternatives to traditional banking channels. The local insurance and asset management sectors are also very interested in fintech solutions. Domestic banks have also started seeing fintech as a way to innovate their everyday business, and have made investments that take advantage of fintech solutions in relation to open banking, cloud

computing, AI, robo-advice, automated systems aimed at increasing the efficiency of internal procedures governing banking and financial services’ compliance, and audit and AML functions, among others.

Combined with the increasing interest expressed by the European and Italian regulators in the sector, fintech will likely be thoroughly regulated in the short- or medium-term. The European Commission recently took steps in this direction by placing two proposals under consultation, one concerning the establishment of an EU framework for markets in cryptoassets and the other a digital operational resilience framework for financial services (see Section VIII).

Further regulatory changes also arrived with the entry into force of the GDPR and the PSD II. The most significant disruption to the global financial sector is still expected to be from ledger technologies such as blockchain. Although the use of this type of technology is not yet widespread, it is expected to emerge in Italy in many areas and, in light of the newly introduced definitions of DLTs and smart contracts, looks set to go beyond cybersecurity and cryptocurrencies.

Finally, although the macro-economic consequences of the covid-19 outbreak and its impact on the Italian financial sector are yet to be seen, innovation and technology are proving to be extremely helpful in addressing the issues arising from the spread of the coronavirus. This will no doubt bring future benefits also in terms of greater exploitation of high-tech activities and services.
I OVERVIEW

The Japanese government has embarked on a string of legislative amendments and other measures aimed at enabling fintech to contribute to the development of Japan’s economic and financial environment, with the expectation that promoting innovation will lead to improved convenience for users and strong growth for companies. As businesses work on creating new financial services that improve users’ convenience and productivity through the use of data, a proactive regulatory response to the efforts of various players is essential, while taking into account the risk of new services. In light of this, Japanese regulators have accelerated the promotion of data utilisation and innovative businesses. They are further developing functional and cross-sectional financial intermediary regulations that cover financial platform providers.

Fintech companies, including start-ups, are also actively engaged in initiatives such as making policy recommendations and setting up self-regulation by forming industry associations and pursuing dialogue with existing financial institutions and the government. The new brokerage legislation, which is scheduled to be enacted in 2020, responds to industry demand. This new rule will allow financial service intermediaries to engage in cross-industry intermediary services in banking, securities and insurance under a single licence.

As a general reference resource about fintech in Japan, the Fintech Association of Japan (an industry association composed of fintech companies, financial institutions, and other related parties) provides a broad introduction to Japanese fintech companies on its English website.²

II REGULATION

i Licensing and marketing

Regulatory overview

Like other jurisdictions, the legal framework of financial regulations in Japan has been fragmented. Specifically, there are: (1) for the products and services layer, licences for designing and providing the products and services, such as banking, insurance, settlement, and remittance; (2) for the sales and marketing layer, licences for selling and marketing the corresponding products and services; and (3) for the infrastructure layer, regulations such

---

1 Atsushi Okada and Takane Hori are partners and Takahiro Iijima is an associate at Mori Hamada & Matsumoto.
2 http://fintechjapan-support.com/nikkei_en/.
as on money laundering regulations and personal information protection. As shown below, a cross-sectional intermediary licence will likely be introduced in banking, securities and insurance.

<table>
<thead>
<tr>
<th>Products/services layer</th>
<th>Banking services</th>
<th>Settlement services</th>
<th>Remittance services</th>
<th>Exchange services</th>
<th>Lending services</th>
<th>Investment services</th>
<th>Insurance services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking services</td>
<td></td>
<td>Prepaid payment instruments; credit; credit-purchasing intermediaries</td>
<td>Fund transfer services</td>
<td>Crypto asset exchanges</td>
<td>Moneylending businesses</td>
<td>Type I/II financial instruments (including security tokens) businesses; investment management services;</td>
<td>Insurance businesses</td>
</tr>
<tr>
<td>Sales/marketing layer</td>
<td>Bank agency services; electronic settlement agency services</td>
<td>Crypto asset exchanges</td>
<td>Moneylending businesses</td>
<td>Financial instruments brokerages</td>
<td>Financial services intermediaries</td>
<td>Insurance agents or brokers</td>
<td></td>
</tr>
<tr>
<td>Infrastructure layer</td>
<td>Money laundering regulations and personal information protection regulations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In principle, the FSA grants and supervises licences for fintech enterprises (e.g., crowdfunding operators, cryptoasset exchanges, and electronic settlement agents) in addition to traditional financial institutions (e.g., banks, insurance companies and financial instruments business operators).

However, for credit card issuers (instalment sales), acquirers and payment service providers (PSPs), licensing and supervision are performed by the Ministry of Economy, Trade and Industry.

ii Services

Banking services

It is necessary to obtain a banking services licence to engage in accepting deposits together with lending funds or discounting bills as a business, or to engage in fund transfer transactions as a business.

Bank agency services

For operators to engage in agency or intermediary services for banking transactions as a business as entrusted by a bank, they must obtain permission to engage in bank agency services. For financial services intermediary business proposed in 2020, see below.

Electronic settlement agency services

Until 2017, when the Banking Act was amended, Japan did not have any regulations in place for services where operators, as entrusted by customers, instruct banks to perform fund transfer transactions, or conduct services to obtain account information and provide it for clients (known as ‘account aggregation’). Since 1 June 2018, the Banking Act requires registration as electronic settlement agents for them to conduct these services as entrusted by
customers. This is a regulatory framework established to cover operators as equivalent to the payment initiation service providers and account information service providers under the EU Payment Services Directive 2 (PSD2).

Payments (settlement and remittance)
Registration or notification is necessary for non-banks to engage in certain types of payment services, including: fund transfer transactions; issuances of prepaid payment instruments (e.g., electronic money and gift vouchers); credit purchase intermediation (e.g., issuance of credit cards); and acquirer or PSP operations. See Section IV.

Cryptoasset exchanges
In 2016, the Payment Services Act (PSA) was amended to include new regulations on cryptocurrency (from 2020, cryptoasset) exchange businesses. Buying and selling cryptoassets (that mainly cover what are called ‘currency tokens’ or ‘payment tokens’) or exchanging them with other cryptoassets is regarded as cryptoasset exchange business, for which cryptoasset exchanges must obtain registration from the local finance bureau. From 1 May 2020, the revised PSA will change the term from ‘cryptocurrency’ to ‘cryptoasset’ and impose stricter regulations on cryptoasset exchanges. See Section V.

Lending
To provide moneylending and intermediary services, a business must obtain registration as a moneylending business. As described in Section IV below, registration as a moneylending business is also required to operate loan-type crowdfunding (crowd-lending or peer-to-peer lending).

Investments
The Financial Instruments and Exchange Act (FIEA) applies to investments in securities and derivatives transactions.

Type I/II financial instruments businesses
Under the FIEA, securities are classified as highly liquid ‘Paragraph 1 securities,’ such as stocks and share options, or ‘Paragraph 2 securities,’ such as fund equities. Broadly speaking, registration as a type I financial instruments business is necessary to purchase and sell Paragraph 1 securities or to act as an intermediary, broker or agent for the sale and purchase of such securities, and to register as a type II financial instruments business is necessary to trade Paragraph 2 securities or to act as an intermediary, broker, or agent for the sale and purchase of such securities.

The amendment of the FIEA in 2014 resulted in some deregulation, and it became sufficient to obtain a more relaxed licence if the operator is only engaged as a business in crowdfunding in which a certain small amount of funds is gathered via the internet (see Section IV).

The amendment of the FIEA in 2019, which will come into force on 1 May 2020, includes security tokens (‘electronically recorded transferable rights’ (ERTRs)) in Paragraph 1 securities. See Section V.
Investment management services
Under the FIEA, operators must obtain registration as investment management services operators in order to manage assets by executing discretionary investment contracts with investors who entrust them with the discretion to make investment decisions. Investment management business operators assume a fiduciary duty and duty of loyalty toward investors, and are subject to regulations regarding conduct, such as an in-principle prohibition on engaging in conflict-of-interests transactions, and prohibition on compensating investors for losses.

Investment advisory and agency services
To provide advice on investment decisions as a business without being entrusted by clients with the discretion to make the actual investment decisions, operators must obtain registration to provide investment advisory and agency services.

Financial instruments brokerages
In addition, business operators entrusted by Type I financial instruments business operators or investment management services operators to act as intermediaries or the like to trade in securities or market derivatives transactions are required to obtain registration as financial instruments brokerages.

Insurance
Insurance businesses
Operators must obtain a licence as an insurance business operator to engage in underwriting insurance as a business.

Insurance agents or brokers
In order to solicit and sell insurance as a business as entrusted by insurance companies, registration as an insurance agent must be obtained. Conversely, to negotiate with insurance companies and act as intermediaries for the conclusion of insurance contracts as entrusted by clients, registration as an insurance broker must be obtained.

Financial services intermediaries
In March 2020, bills were submitted to replace the Financial Instruments Sales Act with the Financial Services Intermediary Act to create a financial services intermediary business. A financial services intermediary business is a licence that allows an intermediary to provide cross-sectional brokerage services in the fields of banking, securities and insurance under a single registration, as opposed to the current system of registration for agents and brokers in each field. If certain requirements are met, registration for electronic settlement agency services is also not required. This new licence will only allow financial services that do not require a highly complex explanation (e.g., brokerage of unlisted stocks and derivatives are prohibited). In order to ensure compensation for damage to customers, a financial services intermediary business requires a deposit. Obligations and prohibited acts will be set depending on the characteristics of the financial services.
iii Cross-border issues

Applicability of Japanese regulations to foreign business operators

Since the purpose of Japan's financial rules is to protect Japanese consumers, operators are in principle subject to the application of Japanese laws and must obtain a Japanese licence when seeking to provide financial services.

In addition, under Japanese financial rules, in principle, a licence cannot be obtained unless the company is governed by the laws of Japan (for licences permitting individuals to perform services, the individual must be a resident of Japan) when providing various types of financial services to Japanese consumers.

However, examples of foreign corporations with business establishments in Japan that are permitted to obtain Japanese licences include type I and II financial instruments business operators, investment management service operators, investment advisers and agents, third-party prepaid payment instrument issuers, acquirers and PSPs.

In addition, examples of foreign corporations that have a foreign licence corresponding to a Japanese licence for financial services, by obtaining a licence in Japan under certain conditions, and are allowed to provide financial services in Japan include banks, insurance companies, fund transfer service providers and cryptoassets exchanges. However, to obtain a licence in Japan, they must satisfy certain requirements, such as having a business office in Japan and a representative in Japan (who is a Japanese resident).

Regulations on foreign ownership

Foreign companies are not prohibited from owning shares or equity in financial-related businesses, including fintech companies. If a foreign company acquires shares or equity in a financial-related business operator, including fintech companies, it is required to submit a report to the authorities through the Bank of Japan in accordance with the Foreign Exchange and Foreign Trade Act.

In addition, other individual laws regulate shareholders (major shareholders) who own more than a certain percentage of their equities. Shareholders holding at least 20 per cent of the equity of a bank or insurance company (in certain cases, 15 per cent) are required to obtain authorisation under the Banking Act or Insurance Business Act. In addition, shareholders holding 20 per cent or more of the shares of financial instruments business operators (in certain cases, 15 per cent or more) are required to file a notification in accordance with the FIEA, and the eligibility of major shareholders is also examined in the registration of financial instruments business operators. In the event that a foreign company is a shareholder, the authorisation of major shareholders and registration examination of financial instruments business operators will include examinations into whether the influence of the foreign company will harm the soundness of Japan's financial services business operators and its financial system.

III DIGITAL IDENTITY AND ONBOARDING

i Digital identity

In Japan, the Public Identity Verification Act provides a structure for personal authentication using e-certificates. In order to use the public identity verification service, individuals must apply at a local government office to receive an individual number card (a ‘My Number’ card). My Number is a 12-digit number assigned to all people (including non-Japanese) who
are registered with their local governments as residing in Japan. It is an individual number introduced to improve the efficiency of administration and convenience for the public by managing personal information in different administrative areas, such as social security and tax, using a common number.

The use of this service was formerly limited to administrative procedures such as tax returns and registry applications, but recent amendments to the Public Identity Verification Act have made it possible for private businesses certified by the Minister of Internal Affairs and Communications to use the service. This may expand the use of the public identity verification service to online account services such as online shopping and banking.

However, at present, the service is not widely used in the private sector due to the lack of widespread use of My Number cards and the need for users to prepare IC card readers or similar devices for reading e-certificates.

ii Digitised onboarding of clients

Until 2018, in order for financial service business operators to confirm their clients’ identity through non-face-to-face transactions, such as those conducted online, they were required to adopt one of the following methods. Mailing procedures were necessary in most cases and therefore know-your-customer procedures were not completed by the digital method alone.

Mailing a copy of identity confirmation documents

A copy of the identity confirmation documents is sent by the client (not limited to post) and the transaction-related documents are mailed by registered post to the client’s residence.

Use of personal receipt post

Transaction-related documents are mailed to the client’s residence by personal receipt post. In this case, the postal service provider confirms the client’s residence and receives a document to confirm the client’s identity.

Use of electronic signatures

Although confirmation of a person’s identity by authentication using an electronic signature is permitted, it has not been widely adopted since the user must obtain a digital certificate in advance and prepare an IC card reader or other similar device.

Use of public identity verification service

Formerly limited to use by administrative agencies, the public identity verification service is now available to private businesses and accepted as a method of identification by financial institutions. However, it is not generally popular since the user must obtain a My Number Card in advance and prepare an IC card reader or other similar device.

Introduction of eKYC procedures

The FSA, together with industry associations, established a working group to examine online transactions in June 2017. The working group discussed ways to realise a more efficient digitised onboarding of clients. Based on the results of such discussions, Japanese anti-money laundering laws and regulations were amended in 30 November 2018 to make customer identity verification methods more flexible through electronic methods for non-face-to-face transactions. New KYC procedures that were introduced include:
transmission of the picture of the identity confirmation documents (attached with a face photo) and the picture of the customer’s appearance; and

transmission of the IC information and the picture of the customer’s appearance.

IV  DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i  Payment services

Registration or notification is necessary for non-banks to engage in certain types of payment services, including: remittances (fund transfer transactions); issuances of prepaid payment instruments (e.g., electronic money and gift vouchers); credit purchase intermediation (e.g., issuance of credit cards); and acquirer or PSP operations.

ii  Funds transfer services

To mitigate the significant burden of obtaining a banking services licence, the PSA, established in 2010, made it possible to make small-amount fund transfers of ¥1 million or less through a single remittance instruction by obtaining registration as a fund transfer service provider without obtaining a banking services licence. As of 29 February 2020, there are 74 businesses registered as fund transfer service providers in Japan.

The bill to amend the PSA was proposed in March 2020 to change the regulations of the fund transfer services. In particular, the bill proposes that the current fund transfer service, which can only handle remittances of ¥1 million or less, should be divided into three types. The Type I fund transfer service would allow authorised providers to transfer money in excess of ¥1 million. This type is based on the needs of overseas remittances. The providers would generally not be allowed to retain customer funds or to accept funds without specific remittance instructions in order to protect customers in the event of their bankruptcy. The Type II fund transfer service would maintain the current fund transfer services framework. The Type III fund transfer service would allow providers to handle transmittance with just tens of thousands of yen, while segregated accounts would be allowed, which provide less safeguarding of customer assets than the other types.

On a separate note, in relation to the payment of compensation for goods and services, ‘billing agency services’ (whereby a business operator receives payment of such consideration on behalf of a goods or service provider (a payee) and delivers the received funds to such payee) are not considered to fall under the definition of ‘funds transfer’ in Japan and thus do not require registration as fund transfer service providers. Many businesses, such as convenience stores, provide these services. The proposed amendment to the PSA in March 2020 clarifies that the services that transfer money among individuals (such as sharing payment apps) are subject to the regulation as money transfer businesses. On the other hand, most of the above conventional billing agency services that accept payments incidental to commercial transactions as agents are expected to remain out of the scope of the money transfer services.

Issuances of prepaid payment instruments

The PSA regulates issuers of prepaid payment instruments to protect consumers and help establish safe and sound payment and settlement systems. Issuers distributing prepaid payment instruments used to pay for goods or services offered by the issuers and third-party merchants (‘third-party type’ prepaid payment instruments) must register with the local finance bureau having jurisdiction over the issuer.
If the prepaid payment instruments are used only to pay the issuer ('own business type' prepaid payment instruments), the issuer must file a notice with the local finance bureau when the unused balance of the prepaid payment instruments exceeds ¥10 million on a reference date (each of 31 March and 30 September).

Furthermore, all issuers of prepaid payment instruments must reserve at least 50 per cent of the total amount of the issuance once the unused balance exceeds ¥10 million as of either reference date. Except for certain cases, the issuer may not redeem or buy back the instruments.

Under the PSA, prepaid payment instruments must have all of the following three elements: record of value; issuance in exchange for consideration; and use as payment or demand. If the instrument satisfies certain exception criteria, such as having a usage period limited to six months or less, it will not constitute a prepaid payment instrument and will be exempt from application of the PSA.

Credit cards, acquirers and PSPs

Japan requires credit card issuers (irrespective of whether they issue physical cards) to be registered as ‘comprehensive credit purchase intermediaries’. The amendment of the Installment Sales Act (ISA) came into force in June 2018, by which (1) acquirers that acquire and manage the merchants who use credit cards; or (2) certain types of payment service providers (PSPs) that enter into contracts with merchants to permit the handling of credit cards, became required to be registered. These services are subject to several obligations, such as proper management of customer credit card numbers. PSPs are not required to be registered if the acquirers have the final decision to conclude merchant agreements and the PSPs’ operations are limited to only the first stage examination of whether to conclude the agreements.

The bill to amend the ISA proposed in March 2020 responds to diverse payment services and providers with the progress of payment technology. For instance, it proposes less strict registration than credit card issuers for services that provide small amounts (ten thousand yen in total) of post-payment services. In addition, the bill allows credit card issuers to use advanced and diverse screening methods to calculate a customer’s payment capacity using their accumulated data. Further, the bill requires broader services, such as QR code payment service providers, to manage customer credit card numbers properly.

Collective investment schemes

The FIEA lists specific forms of instruments as securities. If a product or service (including tokens) falls within any of these securities, then the FIEA regulations apply. In addition to this list, the FIEA also comprehensively defines what is called a ‘collective investment scheme’ (CIS) in order to regulate various types of funds (including foreign funds), regardless of their legal form. CIS arrangements must have all of the following elements:

- monetary contribution (or monetary equivalent) from investors;
- business using the contributions; and
- investors’ entitlement to the distribution of profits arising from the business or of assets relating to the business.

As described below, investment equity interests in investment-type crowdfunding (crowd-lending or peer-to-peer lending) and tokens may be considered CIS equity interests.
For CIS equity interests, subject to some exceptions, registration under the FIEA is required for solicitation for acquisition of the equity interests and management of the assets invested.

Issuers of CIS equity interests are, in principle, required to be registered as type II financial instruments businesses in order to solicit the acquisition of such equity interests.

To manage the assets invested in the fund by the CIS equity interest holders, the issuer must obtain registration as an investment management business in principle.

iv Crowdfunding

In Japan, crowdfunding is classified into ‘donation-type’, ‘purchase-type’, ‘loan-type’ and ‘investment-type’ crowdfunding. A licence is not required to engage in crowdfunding as a business in cases such as ‘donation-type’ crowdfunding (where users donate funds without receiving any consideration in exchange) or ‘purchase-type’ crowdfunding (where users receive products or services in exchange for their funds).

**Loan-type crowdfunding (crowd-lending and peer-to-peer lending)**

Loan-type crowdfunding (crowd-lending or peer-to-peer lending) involves crowdfunding business operators who intermediate between users and parties seeking funds, and such operators must obtain registration as moneylending businesses. The business operators typically solicit funds for loans from the public in the form of investments in fund vehicles and lend such funds to fund users. In order to engage in loan-type crowdfunding, as a general rule, the operators must register as type II financial instruments businesses to solicit investments in the fund, and they must also register as moneylending businesses to provide loans.

**Investment-type crowdfunding**

Investment-type crowdfunding is divided into investments in (1) more highly liquid ‘Paragraph 1 securities’, such as stocks and share options, and (2) ‘Paragraph 2 securities’, such as equity interests in funds.

Prior to the FIEA amendment in 2014, operators had to obtain registration as type I financial instruments businesses in order to trade in or perform brokerage, intermediary, and agency services to trade paragraph 1 securities, and registration as type II financial instruments businesses in order to conduct brokerage and agency services for the sale and purchase of paragraph 2 securities, irrespective of whether a crowdfunding transaction, in which only a small amount of funds is collected, was conducted.

Following the FIEA amendment in 2014, the regulations were relaxed so that operators who only engage in crowdfunding where a certain small amount of funds are collected through the internet can obtain a more relaxed registration as a ‘small-amount electronic public offering business’. However, at present, there are few advantages to being registered as such a business, so many businesses registered as type I or type II financial instruments businesses engage in crowdfunding businesses in conjunction with other businesses.

If a fund intends to invest in real estate, additional rules under the Real Estate Specified Joint Enterprise Act have applied, which made it difficult for funds to invest directly in real estates. In December 2017, the revised Act came into force, which mitigated the regulations, such as allowing for funds to provide online disclosure documents. Real estate investment crowdfunding is expected to boom following this revision.
V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

i Types of cryptocurrencies (cryptoassets) and initial coin offerings
Under Japanese law, businesses that issue, sell and exchange tokens, including token issuances through initial coin offerings (ICOs) or security token offerings (STOs), may fall under the regulations of the PSA or FIEA depending on how they are structured. Businesses involved in ICOs or STOs should adequately fulfil their duties required by related laws and regulations, such as registration when their services are regulated by those Acts.

Under current Japanese law, tokens are likely to fall under the regulatory categories of cryptoassets under the PSA (payment tokens), prepaid payment instruments and securities (especially ERTRs, security tokens). The regulatory framework under the revised PSA and FIEA that will come into effect on 1 May 2020 is described below.

ii Cryptoasset exchange businesses (payment tokens)
The PSA defines cryptoassets and regulates cryptoasset exchange businesses. Current prevailing payment tokens, such as Bitcoin and Ethereum, fall under cryptoassets in the PSA.

Definition of cryptoasset under the PSA
The PSA defines a cryptoasset as electronically recorded proprietary value other than legal currency and assets denominated in any legal currency that:

a can be used to pay unspecified persons for goods and services, can be mutually exchanged into fiat currencies with unspecified persons, and is transferrable through an electronic network (type I cryptoasset); or

b is mutually exchangeable with a type I cryptoasset between unspecified persons and is transferrable through an electronic network (type II cryptoasset).

Cryptoasset exchanges
A ‘cryptoasset exchange business operator’ means one that engages in the business of: (1) selling and purchasing cryptoasset or exchanging cryptoasset with another cryptoasset; (2) acting as an intermediary, broker, or agent for the services in item (1); or (3) managing the monies or cryptoassets of users in connection with items (1) or (2).

Cryptoasset exchanges must manage the funds and cryptoassets deposited by users separately from the operators’ own funds and cryptoassets. As of 30 March 2020, there are 23 companies registered as cryptoasset exchanges in Japan. The FSA did not accept registration of the applicant exchanges and strengthened its role in supervising and inspecting cryptoasset exchanges in 2018, but has gradually restarted the examination process. In 2018, two major cryptoasset-related businesses industry groups merged and set up strict self-regulations to restore public and regulatory confidence in cryptoasset business.

New regulations on cryptoassets
The environment surrounding cryptoasset faced several issues in 2018, including multiple cases of theft of customer assets from cryptoasset exchanges, the realisation that internal control at cryptoasset exchanges was not keeping pace with the sudden increase in transactions, cryptoassets becoming a source of speculative trading owing to wildly fluctuating prices, and
the appearance of new types of transactions using cryptoasset such as ICOs and derivatives transactions. Based on these issues, the PSA and FIEA were amended in 2019, which will come into effect on 1 May 2020.

The revised PSA replaced the term ‘cryptocurrencies’ with ‘cryptoassets’, which mainly covers payment tokens. It also obliges cryptoasset exchanges to address the risk of cryptoasset theft (such as requiring exchanges to maintain both net assets and cryptoassets in an amount equal to or greater than customer cryptoassets stored in ‘hot wallets’, to ensure that the customer right to claim return of cryptoassets is not subject to subordination, and to disclose financial statements), and seeks to strengthen regulations aimed at ensuring appropriate operations (such as requiring public disclosure of transaction price information, prohibiting advertisement or solicitation that encourages speculative trading, and requiring exchanges to notify the regulator before changing which cryptoassets they handle).

Further, it widens the scope of cryptoasset management regulations and anti-money laundering regulations also to cover custody services for cryptoassets, requiring them to be registered.

The revised FIEA covers several features of cryptoasset transactions that need securities-like regulations. For instance, similar to regulations governing the shares of listed companies, the revised FIEA introduces regulations against unfair transactions of cryptoassets. These regulations would prohibit behaviour such as improper activity on cryptoasset transactions, the spreading of rumours and market manipulation, and impose obligations on cryptoasset exchanges to screen transactions. The revised FIEA also regulates cryptoasset derivatives transactions, as in the case of foreign exchange margin trading. It requires registration for exchanges that provide cryptoasset derivatives businesses and introduces similar regulation to foreign exchange margin trading.

iii Financial instruments businesses (security tokens)

The revised FIEA includes security tokens (ERTRs), except for certain less liquid tokens, in Paragraph 1 securities. Therefore, the issuance of security tokens, including STOs, is subject to disclosure and registration obligations under the FIEA. Public placement of ERTRs requires an issuer of ERTRs to file a registration statement and circulate an offering memorandum. Private placement to qualified institutional investors will mitigate the disclosure requirements.

As for registration, in order to register as a type I financial instruments business it is necessary to purchase and sell ERTRs or to act as an intermediary, broker or agent for the purchase and sale of ERTRs (including public and private placement). If an ERTR issuer itself solicits their ERTRs to investors, such an issuer will also likely be required to register as a type II financial instruments business. However, if such solicitation falls under certain private placement (an exempted solicitation to qualified institutional investors and a limited number of accredited investors), simply filing is required instead of registration.

ERTR transactions, including STOs, would also be subject to regulations concerning unfair transactions equivalent to those governing traditional securities.

VI INTELLECTUAL PROPERTY AND DATA PROTECTION

i Intellectual property

In principle, the ideas themselves that pertain to business models are not protected by intellectual property rights such as patent or copyright. However, inventions in which such ideas are realised using information and communication technology may enjoy patent
In regard to software, the Patent Act defines ‘products’ as a concept that includes ‘programs, etc.’, which means that software is subject to patent protection and can be copyrighted. In addition, information that companies manage as trade secrets will be protected under the Unfair Competition Prevention Act.

There have also been patent-related disputes that have attracted attention such as a patent infringement suit in which two leading venture companies in the fintech industry battled over an accounting software algorithm that automatically determines the category of accounting items (Tokyo District Court case of 27 July 2017).

For inventions created by employees, the right to obtain a patent may be assigned to or originally acquired by the employer in accordance with its internal rules. Such employers shall compensate their employees in accordance with such rules; provided, however, that if the rules are found to be unreasonable, the court may decide the compensation in light of the profits arising from the exclusive rights and employer’s contribution to an invention.

The right to file patent applications on inventions made by independent contractors is held by the contractor, unless otherwise agreed between the parties.

ii Data protection

As in other industries, compliance relating to data protection and security is an important issue for fintech businesses. In regard to data protection, the Act on the Protection of Personal Information (APPI) imposes certain obligations on private businesses that use personal information to, for instance: undertake necessary and appropriate measures to safeguard personal information; not use personal information except to the extent necessary for the purposes disclosed to the subject individuals; not disclose personal information data to any third party (subject to certain exemptions); and conduct necessary and appropriate supervision over employees and contractors.

The first significant amendment to the APPI came into force on 30 May 2017 to eliminate ambiguity in the scope of personal information and facilitate the proper use of anonymised data. The fintech industry is also subject to the application of the ‘Guidelines for Personal Information Protection in the Financial Field’. Further, the Personal Information Protection Commission has announced a bill to amend the APPI in March 2020 based on its three-year review, which will likely be enacted within 2020.

In regard to security, the FSA supervisory guidelines governing financial institutions emphasise the importance of matters such as being aware of system risks and enhancing cybersecurity, and operators are required to appropriately follow the PDCA cycle of ‘Plan, Do, Check and Act’.

VII YEAR IN REVIEW

The following events that occurred from late 2018 to present in relation to the development of regulations and legal approaches regarding fintech in Japan are of particular importance.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2018</td>
<td>The FSA released ‘Strategic Directions and Priorities’ and ‘Progress and Assessment of the Strategic Directions and Priorities’.</td>
</tr>
<tr>
<td>November 2018</td>
<td>The anti-money laundering regulations were amended, by which e-KYC was introduced.</td>
</tr>
<tr>
<td>January 2019</td>
<td>The financial system study group of the FSA released a white paper, based on which the revision bills were proposed that allow financial institutions to utilise data that they obtain and introduce a new approval system for ‘insurance business innovation companies’ to be held as subsidiaries of insurance companies.</td>
</tr>
</tbody>
</table>
March 2019 | Bills to amend the PSA and FIEA were proposed, in accordance with the white paper released by the cryptocurrency exchanges study group of the FSA.
---
March 2020 | Bills to amend the PSA to introduce new types of fund transfer services and establish the Financial Services Intermediary Act to introduce financial services intermediary business were proposed. A bill to amend the ISA to introduce less strict registration for small-amount post-payment services and allow credit card issuers to use advanced and diverse screening methods to calculate a customer’s payment capacity was proposed.
---
On 1 May 2020 | The revised acts proposed in January 2019 and March 2019 above will come into effect.

VIII OUTLOOK AND CONCLUSIONS

The following are some of the major legal and regulatory initiatives and developments that are expected in Japan based on the latest financial administrative policy announced by the FSA.

i  Studies into revising the legal framework to make it functional and cross-sectional

From November 2017, sessions of a financial system study group have been convened at the FSA to examine revising the legal framework relating to the financial system (which, as described in Section II above, is currently differentiated by ‘business’ type) to one that is cross-sector and differentiated by ‘function’.

Based on the content of its interim report published in June 2018, the study group has been engaged in discussing the following matters:

a  how to promote appropriate utilisation of information;
b  how to design a legal framework for the payment services area;
c  how to address the emergence of platform businesses under a functional and cross-sectional financial regulatory system; and
d  revising the regulations that govern banks and banking groups.

The study group issued a report in January 2019 summarising the results of issues discussed thus far, including a proposal that banks, insurance companies and Type I financial instruments business operators be permitted to provide services that utilise data obtained from customers. From the perspective of improving sophistication and user convenience in the insurance business, the report stated that it would be appropriate for ‘insurance business innovation companies’ to be held by insurance companies as subsidiaries, as in the case of ‘banking business innovation companies’ that banks are allowed to own as their subsidiaries. The revised acts based on this proposal will come into effect on 1 May 2020.

The study group subsequently considered introducing cross-sectional financial intermediary services. In March 2020, bills were submitted to replace the Financial Instruments Sales Act with the Financial Services Intermediary Act to create a financial services intermediary business and to revise the PSA to introduce new types of fund transfer services. For financial services intermediary business, see Section II.ii. For new fund transfer services, see Section IV .ii.

ii  Policy to enable fintech to lead development of Japan’s innovation environment

With the view that pursuing open innovation (collaboration and coordination) between financial institutions and fintech companies is important to promoting innovation, the Japanese government has been reviewing various systems, such as: developing environments
aimed at the adoption of open APIs; strengthening support for starting new financial businesses and services through initiatives such as a fintech support desk and fintech proof-of-concept hub; and revising methods of customer identity verification for non-face-to-face transactions and examining bank agency service issues.

On 9 March 2018, a cabinet office ordinance was released prescribing detailed rules concerning the amended Banking Act in relation to electronic settlement agents and open APIs, and a guideline was also released indicating the government’s interpretation as to whether such activities constitute bank agency services. Hundreds of banks and other financial institutions are going to promote open APIs at the time of writing and this is anticipated to help promote open innovation between financial institutions and fintech companies in Japan.

In November 2018, amendments to the Japan’s anti-money laundering regulation introduced new e-KYC methods for remote transactions, permitting the use of video chat and facial recognition as well as the use of APIs for verifying financial institution details. It is anticipated that these changes will promote the adoption of e-KYC and lead to frictionless procedures for the opening of accounts.

From 2018 to 2019, several projects have been selected as the first projects to receive assistance through the FSA’s fintech proof-of-concept hub and approved under the newly introduced regulatory sandbox in Japan. The government also plans to actively work on providing sandbox infrastructure in the future.

iii IT governance and cybersecurity at financial institutions

The Japanese government is working to accumulate insight on IT governance in the financial and non-financial industries and further examine better methods of IT governance. In order to further enhance the stability of the financial system as a whole, the government is also seeking to strengthen the cybersecurity measures of financial institutions and working with authorities in various countries to contribute to the formulation of detailed cybersecurity policies.
I OVERVIEW

In recent years, Jersey has made a concerted effort to position itself as a financial technology hub. In 2015, legislation was introduced that exempted virtual currency exchanges with a turnover of less than £150,000 from certain anti-money laundering (AML) requirements to encourage innovation from start-ups in the sector. In 2018, significant progress was made in respect of virtual token offerings (including security token offerings (STOs) and initial coin offerings (ICOs)), and the states of Jersey and the Jersey Financial Services Commission (JFSC) have shown a strong willingness to engage constructively with new forms of fundraising. In the past 12 months, Jersey has seen significant growth as a jurisdiction investing in asset classes connected with the cultivation and processing of medicinal cannabis.

II REGULATION

i Licensing and marketing

Financial services business

The JFSC oversees the regulation of financial services on the island. Anyone wishing to conduct financial services business or deposit-taking business in or from within Jersey will need to register with the JFSC, unless an exemption applies. The JFSC prepares and issues codes of practice that set out both broad principles and detailed requirements to which financial services business in Jersey must adhere. Financial services businesses carrying on regulated activities in or from within Jersey must be authorised to do so by the JFSC, unless an exemption applies.

Article 2 of the Financial Services (Jersey) Law 1998 (FSJL) defines ‘financial services business’ as follows:

A person carries on financial service business if by way of business the person carries on investment business, trust company business, general insurance mediation business, money service business, fund services business or AIF services business.

The most likely of these categories to be relevant to financial technology businesses are investment business and money service business. We have set out the basic definitions below but, depending on the specific facts of a case, there are various exemptions available that may allow a person to be exempt from the requirement to register under the FSJL.
**Investment business**

A person carries on investment business if that person:

- **a** deals in investments, that is, the person buys, sells, subscribes for or underwrites investments, either as principal or as agent;
- **b** undertakes discretionary investment management, that is, the person decides as agent to buy, sell, subscribe for or underwrite investments on behalf of a principal; or
- **c** gives investment advice, that is, the person gives to persons in their capacity as investors or potential investors advice on the merits of:
  - the purchase, sale, subscription for or underwriting of a particular investment; or
  - the exercise of a right conferred by an investment to acquire, dispose of, underwrite or convert the investment.

The definition of investment is set out in a schedule to the FSJL and includes shares, debentures, instruments entitling to shares or securities, certificates representing securities, units in a collective investment trust, options, futures, contracts for difference, long-term insurance contracts and rights and interests in investments.

**Money service business**

A person carries on money service business if they carry on the business of any of the following:

- **a** a bureau de change;
- **b** providing cheque cashing services;
- **c** transmitting or receiving funds by wire or other electronic means; or
- **d** engaging in money transmission services.

**Bureau de change**

The first category of money service business is bureau de change, which is generally taken to mean an office that allows consumers to exchange one currency for another, and charges a commission for the currency exchange service. There is debate as to whether virtual currencies and digital assets comprise currency, a commodity, goods or services, and a view may need to be taken in respect of the particular virtual currency or digital asset if exchange services are being provided in or from within Jersey.

**Money service business exemption order**

The Financial Services (Money Service Business (Exemptions)) (Jersey) Order 2007 (Exemptions Order) (the MSB Order) sets out certain exemptions from the money service business provisions of the FSJL. These are contained in Article 3(2) of the Exemptions Order (the Full Exemptions). The full text is set out below:

```
A person who carries on money service business consisting of the transmission or receipt of funds by wire or other electronic means, or the provision of money transmission services, by the person for the sole purpose of any of the following:

- **a** enabling another person to pay for goods or services;
- **b** enabling another person to access that other person’s funds or that other person’s money;
- **c** is a prescribed person for the purposes of Article 7(2)(a)(ii) of the [FSJL] in relation to that money service business.
```
Accordingly, persons falling within the Full Exemptions are exempt from the requirements to comply with the FSJL in respect of money service business.

There is no case law and little guidance around the application of the Full Exemptions, but a virtual currency exchange or similar financial technology business may in certain circumstances be able to rely on the Full Exemptions.

**Turnover exemption**

A limited exemption is set out in Article 4 of the MSB Order, which states that a person is exempt from having to register to conduct money service business if:

- that person notifies the Commission in writing that he or she intends to carry on money service business; and
- the turnover for the last completed financial period for the money service business carried on by that person is less than £300,000.

For the purposes of (b), above, after a person first begins to carry on money service business, the turnover for that business shall be taken to be less than £300,000 until whichever of the following dates is earliest:

- the end of the first 18 months after the person begins to carry on the business; or
- the date when the turnover in respect of the business for the last completed financial period is ascertained.

If a person was exempt by virtue of the exemption set out above, and the turnover of that person for the last completed financial period that begins within, or immediately follows, the period for which the person was an exempt person by virtue of the exemption set out above, is more than £300,000, that person shall be an exempt person until:

- 10 months after the end of that person’s last completed financial period for which the turnover is £300,000 or more; or
- if the person is a public company, seven months after the end of the last completed financial period for which the turnover is £300,000 or more.

To the extent that a financial technology business were to engage in money service business, they would be exempt from the requirement to register with the JFSC until their turnover exceeded the £300,000 threshold, as detailed above (but, as noted above, the JFSC will need to be notified irrespective of turnover).

**Virtual currency exchange**

If an entity will be exchanging fiat currency for cryptocurrency (or vice versa) (for example as part of STO or ICO, or as a stand-alone virtual currency exchange), then it will need to consider if it needs to register with the JFSC as a virtual currency exchange. Procedures in relation to AML and countering the financing of terrorism (CFT) will need to be put in place. In practice, where a Jersey corporate services provider (CSP) has been appointed we would normally expect the AML or CFT process to be set up and administered with compliance staff provided by the CSP, rather than by the virtual currency exchange or STO or ICO issuer itself.

While the general rule is that virtual currency exchanges will be required to register with the JFSC, Jersey introduced innovative amendments to Jersey statute in 2015, which created a safe harbour for exchanges with a turnover of less than £150,000 (exempt exchanges).
Exempt exchanges simply have to notify the JFSC that they are exchanging virtual currency, but will not be required to register or pay annual fees to the JFSC. This approach has created a regulatory sandbox, which is targeted at encouraging innovation, allowing new business models, services and products to be tested without undue regulatory burden.

In any event, any person conducting virtual currency exchange business in Jersey will be required to comply with the requirements of the Jersey AML/CFT Handbook. As noted above, in practice this work is often coordinated by and with support from the CSP.

**Control of Borrowing (Jersey) Order 1958**

The Control of Borrowing (Jersey) Order 1958 (COBO) requires that the consent of the JFSC be obtained for various activities, including:

* a to allow a Jersey company to issue shares (in practice this means that every company incorporated in Jersey must have valid COBO consent);
* b to allow a foreign body corporate to register shares or other securities in Jersey;
* c to allow a Jersey company to issue any securities other than shares; or
* d to circulate a prospectus or offer of securities in Jersey.

The JFSC may refuse to grant a COBO consent or may attach such conditions to the COBO consent as it sees fit, and there are a number of exemptions to the above requirements.

**Securities**

COBO contains a broad definition of securities, which includes shares, bonds, notes, debentures and debenture stock. The JFSC has issued a separate guidance note where virtual tokens are issued in connection with an STO or ICO (see below).

**Prospectuses**

An exemption is available from the requirement for a non-Jersey entity to obtain a COBO consent for the circulation of an offer of securities in Jersey where articles 8(2)(a) and 8(2)(b) of COBO are satisfied, as follows:

* a Article 8(2)(a) requires that the body corporate issuing the securities has no relevant connection with Jersey. In summary, any of the following will constitute a relevant connection for the purposes of COBO:
  * the management or administration of the body corporate is wholly or partly carried on in Jersey;
  * control of the body corporate is exercised in or from within Jersey;
  * at the time of the offer, at least one-third of the directors of the body corporate is resident in Jersey;
  * the body corporate has entered into or is about to enter into an agreement with a Jersey resident person material to the offer;
  * a business material to the offer is being carried on by the body corporate in or from within Jersey; or
  * the offer is an offer for exchange of securities issued by a Jersey company or units of a Jersey unit trust scheme; and
* b Article 8(2)(b) requires either that:
  * the offer by the body corporate is not an offer to the public. The offer will not be an offer to the public if it is communicated to no more than 50 persons in Jersey; or
• the offer by the body corporate is a valid offer in the United Kingdom or in Guernsey and is circulated in Jersey only to persons similar to those to whom, and in a similar manner to that in which, the offer is being made in the United Kingdom or Guernsey, as the case may be.

An offer is 'valid in the United Kingdom' if an identical offer is for the time being circulated in the United Kingdom without contravening, effectively, the Financial Services and Markets Act 2000.

**Issuing a prospectus**

The Companies (Jersey) Law 1991 (the Companies Law) is Jersey's primary piece of legislation relating to Jersey companies and sets out the requirements for a Jersey company to issue a prospectus in Jersey. A prospectus is defined as an invitation to the public to become a member of a company or to acquire or apply for any securities, for which purposes:

- an invitation is made to the public where it is not addressed exclusively to a restricted circle of persons; and
- an invitation is not addressed to a restricted circle of persons unless:
  - the invitation is addressed to an identifiable category of persons to whom it is directly communicated by the inviter or the inviter's agent;
  - the members of that category are the only persons who may accept the offer and they are in possession of sufficient information to be able to make a reasonable evaluation of the invitation; and
  - the number of persons in Jersey or elsewhere to whom the invitation is so communicated does not exceed 50.

If a prospectus is being issued by a company in respect of its own securities, the issuing company must be a public company. It is a criminal offence for a private company to issue a prospectus in relation its own securities.

A prospectus must comply with certain content requirements set out in the Companies (General Provisions) (Jersey) Order 2002 (CGPO), and include details of:

- the offer;
- the capital of the issuer;
- any amounts written off or provided for in respect of goodwill or preliminary expenses, or of any benefit given to a promoter;
- material contracts;
- interests of directors;
- debentures and loans of the issuer;
- the company's latest accounts, including notes on any unusual risks to the investor;
- registered office (and principal operating establishments);
- directors and secretary;
- advisers (including the name and address of the issuer's auditors, legal advisers and principal bankers);
- date of issue; and
- any other material information.
Crowdfunding

The JFSC has clarified that in most cases crowdfunding would not be a regulated activity. There are, however, a number of legal considerations to take into account before an entity can engage in crowdfunding. As set out above, the kind of issues that would need to be addressed would be whether a prospectus is required pursuant to the CGPO, or whether additional consents are required pursuant to COBO or whether these would be deposit taking business under the Banking Business (Jersey) Law 1991 (which is outside the scope of this chapter).

ii Cross-border issues

Jersey is a leading centre in the funds industry, which in recent years has included a focus on technology funds. Notably, SoftBank Group raised its US$100 billion Jersey domiciled technology fund in 2016. Jersey has never been a Member State of the European Union, but has put in place all of the infrastructure needed to allow funds and other similar investment structures launched in Jersey to be marketed to both UK and EU investors. Jersey has implemented a voluntary regime that mirrors the requirements of the Alternative Investment Fund Managers Directive (AIFMD). While the full AIFMD passport has not yet been extended to non-EU third countries, Jersey funds are able to market to EU investors through the National Private Placement Regimes of EU Member States.

III ONBOARDING

The JFSC recently updated its AML/CFT Handbook for regulated financial services businesses (the Handbook) to more widely permit evidence of identity to come from electronic sources (E-ID) as an alternative to original ‘wet ink’ documents. E-ID is described in the Handbook as ‘the use of smart phone and tablet applications to capture information, copy documents and take photographs of customers as part of [a relevant person’s] CDD processes’.

The previous version of the Handbook already included guidance on the use of E-ID in CDD processes, which has been retained in the revised version; however, it was not previously clear whether E-ID was an acceptable substitute for wet ink identification documents, or whether it could only be used alongside more traditional forms of due diligence. The changes to the Handbook include the addition of a reference to E-ID in the list of acceptable sources of evidence of identity, alongside original wet ink documents, certified copy documents and external data sources.

This update has proved invaluable during the covid-19 pandemic, allowing clients to be onboarded when the exchange of wet ink documents became difficult or impossible.

IV CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS (ICOS)

The JFSC has published guidance on how ICOs will be approved in Jersey through existing laws and regulation (the Guidance), which has been endorsed by the Jersey government.

As with all Jersey companies (and as set out above), a proposed ICO issuing company will require a consent from the Jersey Companies Registry under COBO), and in considering an application the Registry will have regard to the Registry’s Processing Statement (RPS) and the Sound Business Practice Policy (SBPP). In addition to publishing the Guidance, the JFSC has published updated versions of the RPS and the SBPP to specifically address ICOs, and the approach that the JFSC will take in considering applications to form an ICO issuer in Jersey.
The Guidance provides that, as a general rule, Jersey based ICO issuers will be required to be incorporated in Jersey and administered through a licensed CSP in Jersey.

An application to the JFSC must address whether the tokens are a ‘security’ or not for the purposes of COBO. If the tokens are a security, then absent an exemption an additional consent under COBO will be required for the issue of securities other than shares. If the tokens are not a security, then the additional COBO consent will not be required and the JFSC may consider relaxing some of the conditions that are set out in the Guidance.

In classifying an ICO, the Guidance provides that the JFSC will focus on the economic functions and purpose of the token to be issued and whether the tokens are tradeable or transferable. The definition of security in COBO is broad, and the Guidance states that a token will be considered a security token for Jersey law purposes if it has characteristics usually associated with an equity or debt security, including:

- a right to participate in the profits or earnings of the ICO issuer or a related entity;
- a claim on the issuer or a related party’s assets;
- a general commitment from the ICO issuer to redeem tokens in the future;
- involvement in the ownership or running of the ICO issuer or a related party; and
- expectation of a return of the amount paid for the tokens, with or without interest or other form of gain.

If a token is deemed not to be a security token, it will typically be either:

- a utility token, in other words, a token that merely confers on the holder the right to use or access a product or service, with no economic rights or any right to redeem the token for value; or
- a cryptocurrency token, in other words, the token is designed to behave like a currency, referred to in some jurisdictions as a payment token.

### General requirement for all ICO issuers

To ensure consistency and provide a streamlined COBO application process, the Guidance requires all ICO issuers to:

- be incorporated as a Jersey company (i.e., not be a foundation or limited partnership or other form of vehicle);
- receive a consent under COBO before undertaking any activity;
- apply relevant AML or CFT requirements to persons that either purchase tokens from or sell tokens back to the issuer of those tokens;
- appoint and maintain a duly regulated Jersey CSP;
- appoint and maintain a Jersey resident director on the board of the ICO issuer, where the Jersey resident director is also a principal person or key person of the CSP;
- obtain the JFSC’s prior approval to any change either to the issuer’s administrator or the Jersey resident director of the issuer;
- prepare and file annual audited accounts with the Jersey Companies Registry;
- have procedures and processes in place to (1) mitigate and manage the risk of retail investors investing inappropriately in the ICO; and (2) to ensure retail investors understand the risks involved;
- prepare and submit to the JFSC for its approval an Information Memorandum (which may be in the form of a White Paper) that complies with certain content requirements of a prospectus issued by a company under the Companies (Jersey) Law 1991; and
- ensure that any marketing material (including the information memorandum) is clear, fair and not misleading.
As with all new incorporations, the JFSC has reserved the right to consider each application on its own merits, so while the conditions set out above offer helpful guidance on the approach the JFSC is likely to take, they are by no means definitive.

ii  Jersey legal advice

The Guidance provides that an application under COBO in respect of an ICO issuer must be accompanied by analysis prepared by a Jersey law firm outlining:

a. the proposed activity including relevant timelines;

b. details of the issuer and the ICO;

c. the rationale for the ICO, amount to be raised and use of proceeds;

d. a summary of the features of the tokens;

e. a summary of purchase and redemption processes;

f. service providers to the issuer;

g. the relationship between the issuer and the holder of the tokens;

h. the management of underlying assets and security rights over such assets for holders of the tokens;

i. how the activity will be wound up or dissolved and assets distributed to the holders of the tokens; and

j. a Jersey legal and regulatory analysis considering applicable law and regulation (including laws in respect of investment funds, financial services, banking, AIFMD, proceeds of crime and AML).

iii  CSP requirements

The Guidance provides that, prior to a Jersey CSP agreeing to act as the administrator of an ICO, and on an ongoing basis, it must take steps to satisfy itself as to a number of factors, including:

a. the honesty and integrity of the issuer and the persons associated with it;

b. the issuer’s approach to acting in the best interests and needs of each and all of its customers;

c. the adequacy of the issuer’s financial and non-financial resources;

d. how the issuer will manage and control its business effectively, and ensure that it will conduct its business with due skill, care and diligence;

e. the effectiveness of the issuer’s arrangements in place for the protection of client assets and money when it is responsible for them;

f. the effectiveness of the issuer’s corporate governance arrangements;

g. what systems the issuer has in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing; and

b. the issuer’s marketing strategy, including the types of persons to whom the ICO will be marketed, how it will be marketed, and the jurisdictions in which it will be sold or marketed (including consideration of any relevant laws or restrictions that may apply in other jurisdictions).

The Guidance also summarises the JFSC’s expectations in relation to ICO issuers mitigating the risk of anti-money laundering and countering the financing of terrorism.
iv Retail investors
The Guidance provides that an ICO issuer must take appropriate steps to mitigate and manage the risks of retail investors investing inappropriately in ICOs. In this regard, the Guidance contains a safe harbour process including an approved risk warning that must be actively confirmed by each investor as being understood and accepted.

v Marketing and offer document
All marketing materials must be clear, fair and not misleading, and contain prescribed wording in respect of the role of the JFSC in approving the ICO. In particular, the JFSC does not regulate an ICO issuer as such, although the approval procedure set out in the Guidance mandates a set of conditions designed to ensure that the issuer meets specific standards in terms of governance, investor disclosure, anti-money laundering and countering the financing of terrorism.

The offering document must comply with the content requirements set out in the CGPO, and contain the specific statements set out in the Guidance. In addition, prior to the issuance of any tokens, the JFSC must confirm that it has no objection to the issue of the offer document.

vi Ongoing requirements
The Guidance provides certain ongoing requirements, including:

a. the board of directors of the ICO issuer must notify the JFSC if it defaults on any tokens issued;
b. the board must make an annual filing to the JFSC confirming that there has been no breach of the conditions attached to the consent or consents issued under COBO;
c. the ICO issuer must seek the prior consent of the JFSC to any material change to the matters set out in the application for a consent under COBO; and
d. prior JFSC consent is required for any change in Jersey CSP, or any change in Jersey resident director.

ICO application form
In addition to the Guidance the JFSC has published an application form that potential ICO issuers will be required to complete. The form requires details of:

a. the consent being sought;
b. the corporate services provider;
c. the issuing entity (including details of the ultimate beneficial owners);
d. the issue, including the type of token being issued, a description of the rationale behind the issue and any underlying assets;
e. the legal relationship that will be created between the issuer and holders of the tokens, including a description of how the token holders will benefit from the activity being funded by the ICO;
f. the ICO’s target market;
g. the steps taken to protect purchasers of the tokens;
h. details of who will take responsibility for the contents of the information document or white paper, and whether it will be issued in a language other than English;
i. whether the ICO will comply with the JFSC’s Sound Business Practice Policy;
j. whether the tokens will be securities for the purposes of COBO, or whether the ICO issuer will be carrying on another regulated activity;
whether the issuer will be an AIF for the purposes of AIFMD; and
whether the issuer will also be a virtual currency exchange under the Jersey virtual
currency exchange regime, which was introduced in 2015.

Potential issuers will also be required to complete a memorandum of compliance in a form
 appended to the application form for any information document or white paper produced
in respect of the ICO, which includes a checklist containing various information statements
that must be included pursuant to the CGPO (as described above).

V OTHER NEW BUSINESS MODELS

The Electronic Communications (Jersey) Law 2000 (the Communications Law) was
amended in October 2019 to provide additional clarity that Jersey law-governed documents
can be signed using an electronic signature. The Communications Law allows for contractual
offer and acceptance to take place by way of an electronic communication (which includes
electronic signatures).

The Communications Law gives the attributes of an electronic signature as a ‘signature
in electronic form attached to or logically associated with an electronic communication or
electronic record’.

Where a person is required by statute to provide a signature (for example, pursuant to
the provisions of Jersey companies or securities laws), they will have met that requirement if:

a a method is used to identify the person and to indicate the person’s approval of the
information communicated;

b the method used is as reliable as is appropriate for the purposes for which the information
is communicated; and

c the person to whom the signature is to be provided consents to the method of providing
the electronic signature (consent).

The Communication Law states that an electronic communication would not be sufficient
to effect offer and acceptance in a contract where the law expressly or impliedly provides
otherwise. Certain transactions may require a wet ink signature, or have other formality
requirements, for example, the transfer of Jersey real property.

In addition to providing new sources of business for technology businesses providing
electronic signing services, this has also made doing business easier and more streamlined.
These updates to Jersey law have been particularly helpful in managing the impact of the
disruption caused during the covid-19 crisis, allowing Jersey businesses and counterparties to
continue to transact when exchanging hard-copy documents with wet ink signatures became
in some cases impossible.

VI INTELLECTUAL PROPERTY AND DATA PROTECTION

Jersey has had data protection legislation since 2005. Following the introduction of the
General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED),
Jersey brought in two pieces of legislation to ensure that the Jersey data protection regime
maintains equivalence with the EU data protection laws. The legislation is:

a the Data Protection (Jersey) Law 2018 (DPJL); and

b the Data Protection Authority (Jersey) Law 2018 (DPAJL).
The DPJL deals with duties of data controllers (including the data protection principles), duties of data processors, conditions for processing, obligations to appoint data protection officers, rights of data subjects, exemptions to parts of the law, cross-border transfers and exemptions to the adequacy requirements and remedies and enforcement. Although largely consistent with the GDPR, there are some differences, for example, the period for complying with data subject rights requests is four weeks rather than one month (as is the case in the GDPR) and the right of further extension is eight weeks rather than two months (as is the case in the GDPR).

The DPAJL establishes the data protection authority in Jersey, and includes powers allowing it to investigate complaints and undertake inquiries along with granting it powers of sanction following a finding of a breach (including fines).

VII YEAR IN REVIEW

Following an overhaul of the JFSC’s approach to STOs and ICOs in 2018, 2019 has been a year of consolidation for Jersey’s technology sector. Jersey has seen a steady increase in the number of technology-focused investments structured through the Island, in the form of (among others) ICOs, STOs, joint ventures and funds.

Medicinal cannabis was a significant growth sector in Jersey during the course of 2019. The States of Jersey has shown significant interest in developing the medicinal cannabis industry, and notably recently amended the Misuse of Drugs (Jersey) Law 1978 and the Medicines (Jersey) Law 1995 (Drugs Laws) to create an exemption from the general prohibition on the import, processing and possession of medicinal cannabis in certain circumstances. We understand that a ministerial decision is also under consideration that would allow for a greater concentration of certain trace amounts of controlled substances in cannabidinol (i.e., CBD oil, a legal and widely used substance that is extracted from medicinal cannabis plants) to make extraction of CBD oil easier.

In addition to the boost these measures will give to those directly investing in and involved in the processing of medicinal cannabis, a number of other players in the technology space will also benefit as this growing asset class becomes more widely accepted and legal barriers come down. In particular, following Jersey’s recent updates to the Drugs Laws, financial technology businesses providing, for example, IT services or payment services are likely to find it easier to offer these services from Jersey in light of the reforms without falling foul of the Proceeds of Crime (Jersey) Law 1999.

VIII OUTLOOK AND CONCLUSIONS

Jersey continues to develop as a leading fintech jurisdiction, and has looked to innovate further during the course of this year by developing its medicinal cannabis industry, a key potential source of business for the jurisdiction’s technology businesses.

This innovation builds on Jersey’s existing success in establishing itself as a leading STO and ICO jurisdiction. Jersey’s success as a technology-friendly jurisdiction is underlined by the presence of major global technology businesses calling Jersey home, in particular in recent years, Binance, the world’s largest cryptocurrency exchanger; Global Advisors, a leading crypto fund manager; and SoftBank, the world’s largest technology fund, have established themselves in Jersey.
Chapter 13

LUXEMBOURG

Anne-Marie Nicolas, Álvaro Garrido Mesa and Sandy Brumberg

I Overview

Luxembourg is a reference jurisdiction for the financial services industry and has always been keen to evolve and implement new innovative technologies in the day-to-day business framework. It should be highlighted that Luxembourg recently passed an amendment to the law on the circulation of securities to include the concept of distributed ledger technology such as blockchain.

The LHoFT Foundation, Luxembourg for Finance, Luxinnovation, Digital Luxembourg and ABBL Fintech map constitute useful sources of information.

Luxembourg provides for an attractive IP and tax regime that allows companies to benefit from a tax exemption of 80 per cent on certain types of eligible income streams, and for other incentives such as investment tax credits and government grants for innovative start-ups.

Regarding corporate tax, Luxembourg-resident companies are subject to corporate income tax (CIT) at a rate of 17 per cent on the basis of their worldwide income. However, companies whose taxable income does not exceed €175,000 are subject to a lower CIT rate of 15 per cent. A contribution to the unemployment fund (7 per cent of the CIT charge) and municipal business tax (6.75 per cent in Luxembourg city), i.e., the aggregate corporate tax rate amounts to 24.94. Luxembourg resident companies are also subject to an annual net wealth tax at a rate of 0.5 per cent on the basis of their total net assets (subject to certain exemptions).

Luxembourg has a prominent financial services industry and a unique opportunity to strategically leverage financial investment and services that could facilitate and accelerate the transition to a digitally interconnected economy through enhancing fintech and entrepreneurship. In that respect, Luxembourg Digital Tech Fund has contributed by investing in tech start-ups and supporting cybersecurity, fintech, big data and digital health. In addition, a good example would be Bitstamp, a Luxembourg-based Bitcoin exchange company that has been granted a payment institution licence by the Luxembourg financial supervisory authority (CSSF) and is acting as a payment institution. However, although Luxembourg widely promotes innovation and embraces fintech, and is at the top of the list of fintech-friendly jurisdictions, there are further steps to be taken to ensure a long-lasting implantation of such highly innovative companies.

1 Anne-Marie Nicolas is a partner, Álvaro Garrido Mesa is a senior associate and Sandy Brumberg is a professional support lawyer at Loyens & Loeff Luxembourg Sàrl.
II REGULATION

i Licensing and marketing

In Luxembourg, fintech companies are subject to the following main regulations:

a the Luxembourg Law of 10 November 2009 on payment services, as amended (the 2009 Law);

b the Luxembourg Law of 5 April 1993 on the financial sector, as amended (the 1993 Law);

c CSSF-related regulations and circulars, provided that their activities fall within the scope of the above-mentioned laws;


e the Luxembourg Law of 7 December 2015 on the insurance sector (the 2015 Law);

f the Luxembourg Consumer Code (the Consumer Code); and

g the Luxembourg Law of 14 August 2000 on electronic commerce, as amended.

There is no special fintech licence in Luxembourg. However, activities performed by fintechs may be subject to licensing requirements pursuant to the 2009 Law, the 1993 Law, or the 2015 Law.

In addition, since activities performed by fintechs can be qualified as ‘economic activities’, they may be subject to the prior granting of a business licence.

Fintechs that would like to establish themselves in Luxembourg in order to carry out an activity of the financial sector (e.g., the issuing of means of payments in the form of virtual or other currencies, the provision of payment services using virtual or other currencies, or the creation of a market (platform) to trade virtual or other currencies) must define their business purpose and their activity in a sufficiently concrete and precise manner to allow the CSSF to determine for which status they need to receive the ministerial authorisation.2

Insurtechs and reinsurtechs that would like to establish themselves in Luxembourg in order to carry out an activity of the insurance or reinsurance sectors must submit their project to the Luxembourg Supervisor of the Insurance Sector (CAA).

The business licence is issued to businesses (professionals operating under their own name, or companies) within three months, which may be extended by an additional month in certain cases, if:

a the applicant fulfils the legal conditions for qualification (when required) and professional integrity for the activity concerned; and

b the business has a fixed physical establishment in Luxembourg (no ‘letterbox companies’).

The business licence is required for any person that wishes to engage in the following professional activities as a self-employed person or as a company:

a commercial activity (trade, HORECA (hotel, restaurant and catering sector), transports, industry, etc.);

b craft activity (food, fashion, construction, mechanical engineering, audiovisual, entertainment, art, etc.); or

c certain liberal professions that are mainly intellectual in nature.

---

Undertakings that carry out an activity of the financial sector must obtain an authorisation from the Minister of Finance and are subject to the prudential supervision of the CSSF.

The activity of direct insurance or reinsurance is subject to prior authorisation from the minister with responsibility for the insurance sector through the CAA.

With respect to the business licence, it is granted by the General Directorate for Small and Medium-Sized Enterprises.

Robo-advice

In Luxembourg, digital financial advisory services, in the same manner as traditional financial advice services, are subject to the regulatory requirements of the CSSF. The type of licensing required by a robo-adviser to perform its activities depends on the operating model chosen including the services provided, the contractual arrangements and the structure of the platform. Robo-advisers need to obtain an authorisation as:

a investment advisers: in the same way as traditional, non-automated financial advisers that limit themselves to advisory services and do not intervene in the implementation of the advice provided by them (Article 24 of the 1993 Law);

b private portfolio managers: whenever robo-advisers use the technology to manage portfolios as per client’s mandates on a discretionary client-by-client basis (Article 24-3 of the 1993 Law);

c brokers in financial instruments: when their servicing consists of the role of an intermediary by either encouraging parties to be brought together with a view to the conclusion of a transaction, or in passing on their clients’ purchase or sale orders without holding the investments of the clients (Article 24-1 of the 1993 Law); and

d commission agents: in cases where robo-advisers execute orders on behalf of clients and in relation to one or more financial instruments (Article 24-2 of the 1993 Law).

To obtain a licence, a formal application needs to be submitted to the CSSF. The format of the application varies with the nature of the robo-advice activity envisaged.

Fintechs offering robo-advisers should regularly monitor the effectiveness and appropriateness (in line with MiFID II requirements) of the advice provided to avoid mis-selling. Precautionary mechanisms should be in place to be able to suspend the provision of advice should errors or bias be detected.4

Asset management company

Authorisation to act as a management company is subject to the requirements as set out in the Law of 17 December 2010 relating to undertakings for collective investment (the 2010 Law).


4 Artificial Intelligence, CSSF White Paper, Opportunities, Risks and recommendations for the financial sector, December 2018. This document intends to provide some basic knowledge about artificial intelligence (AI) and describes the different types of AI and some practical use cases for the financial sector. Furthermore, the study covers the analysis of the main risks associated with AI technology and provides some key recommendations to take into account when implementing AI inside a business process.
There are special rules on credit information services (e.g., pre-contractual information, information to be mentioned in the credit agreements, right of cancellation) to comply with those that are detailed in the Consumer Code.

**2009 Law**

Luxembourg payment institutions and electronic money institutions that intend to provide payment services in the territory of another Member State, either through the establishment of a branch, through the use of agents or through the freedom to provide services, are subject to information requirements to be disclosed to the CSSF.

**1993 Law**

Only Prepaid Financial Services (PFSs) belonging in the category of ‘investment firms’ (such as investment advisers, brokers in financial instruments, commission agents and private portfolio managers) can hold a European passport (the EU Passport). 5

On the contrary, specialised PFSs (such as professionals providing company incorporation and management services, professionals performing lending operations and corporate domiciliation agents) and support PFSs (such as client communication agents, primary IT systems operators of the financial sector, secondary IT systems and communication networks operators of the financial sector) may not benefit from the EU Passport. As a consequence, specialised PFSs and support PFSs would need to obtain an authorisation from the competent authority of the host Member State in which they intend to operate.

The EU Passport covers:

a. the investment services listed in Section A of Annex II of the 1993 Law (such as dealing on own account, portfolio management and investment advice); and

b. where appropriate, one or more of the ancillary services listed in Section C of Annex II of the 1993 Law (such as safekeeping and administration of financial instruments for the account of clients, granting credits or loans to an investor to allow him or her to carry out a transaction in one or more financial instruments, or foreign exchange services where these are connected to the provision of investment services).

**ii Cross-border issues**

**2009 Law**

*EU payment institutions and electronic money institutions*

Payment institutions and electronic money institutions for which the home Member State is a Member State other than Luxembourg, may provide payment services or electronic money services in Luxembourg, either through the establishment of a branch or through the engagement of an agent or the provision of services, provided that their activities are covered by their authorisation.

---

5 CSSF Questions and Answers on how to obtain authorisation as PFS, as updated on 24 October 2018, Item 24 Which PFS can hold a 'European passport' and which services fall under this regime?, p.11.
Third-country payment institutions and electronic money institutions

Payment institutions incorporated in third countries wishing to establish a branch in Luxembourg are subject to the same authorisation rules as payment institutions for which Luxembourg is the home Member State. Compliance by the foreign institution with the required conditions for authorisation shall be assessed (i.e., professional standing and experience of the persons responsible for the branch, central administration in Luxembourg and adequate administrative infrastructure in Luxembourg).

1993 Law

EU credit institutions, investment firms and financial institutions

Provided that their activities are covered by their authorisation, EU-based credit institutions, investment firms and financial institutions may exercise their activities in Luxembourg by the way of:

a  the provision of services;
b  through the establishment of a branch; or
c  through the use of a tied agent.

The tied agent is assimilated to the Luxembourg branch and is subject to the provisions of the 1993 Law applicable to Luxembourg branches of EU credit institutions and investment firms.6

EU-based financial institutions may also benefit from the EU Passport provided that they meet certain requirements (such as the financial institution being the subsidiary of a credit institution or the jointly owned subsidiary of several credit institutions).7

Third-country credit institutions and third-country PFS other than investment firms

The exercise of third-country credit institutions (for their banking activities) and PFSs other than investment firms’ activities in Luxembourg requires the establishment of a branch. They are subject to the same authorisation rules as those applying to credit institutions and other professionals governed by Luxembourg law, as respectively covered in the 1993 Law.8

On the contrary, if these third-country firms are not established in Luxembourg but occasionally and temporarily come to Luxembourg to, among other things, collect deposits and other repayable funds from the public and to provide any other service under the 1993 Law, they must hold an authorisation from the Minister responsible for the CSSF.

These third-country firms are subject to equivalent authorisation and supervisory rules to those of the 1993 Law in their home Member State.9

There is no distinction provided in the 2009 Law or in the 1993 Law between the different types of fintech services or products that may be offered from abroad into Luxembourg without a physical presence in Luxembourg.

---

6 Article 30(2) of the 1993 Law.
7 Article 31 of the 1993 Law.
8 Article 32(1) of the 1993 Law.
9 Article 32(5) of the 1993 Law.
Pursuant to both the 2009 Law and the 1993 Law, fintech services or products may be offered from abroad into Luxembourg by an entity without a physical presence in Luxembourg only through the provision of services by EU-based entities (payment institution or electronic money institutions, credit institutions, investment firms or financial institutions).

The establishment of a branch is, however, required if the fintech services or products are offered in Luxembourg from a third-country (non-EU) firm (payment institution or electronic money institutions, credit institutions or third-country PFSs other than investment firms).

Pursuant to both the 2009 Law and the 1993 Law, EU-based entities (payment institution or electronic money institutions, credit institutions, investment firms or financial institutions) do not need to obtain a local licence if they provide cross-border services and products and benefit from the EU Passport to the extent these services are all passportable.

Regarding whether services or products are actively marketed or if the client solicits the service or product, this is only relevant if a third-country firm intends to provide investment services (e.g., investment advice or portfolio management) in Luxembourg. In such case, the 1993 Law distinguishes two situations depending on the clients targeted and whether the provision of the investment service is exclusively initiated by the client, given below.  

First, when targeting eligible counterparties or professionals clients, equivalence and cooperation must be taken into account. In the absence of an equivalence decision of the European Commission taken in accordance with Article 47(1) of the Markets in Financial Instruments Regulation, the third-country firm may also provide investment services in Luxembourg to eligible counterparties and professional clients, provided that the following conditions are fulfilled:

- it is permitted within its jurisdiction to provide investment services and engage in investment activities that it wishes to offer to Luxembourg;
- it is subject to supervision and authorisation requirements that the CSSF considers equivalent to those of the 1993 Law; and
- cooperation between the CSSF and the supervisory authority of this firm is ensured.

Second, when targeting retail clients or clients who may be treated as professionals on request, obligation to establish a branch must be taken into account. If the third-country firm intends to provide in Luxembourg investment services to retail clients or clients who may be treated as professionals on request within the meaning of Annex III, Section B of the 1993 Law, it must establish a branch and is subject to the same authorisation requirements as the Luxembourg credit institutions and investment firms. CSSF approval is granted upon written request and after instruction by the CSSF. The decision taken on an application for approval shall be notified to the undertaking applicant within six months of the submission of a complete application, failing which the absence decision is equivalent to the notification of a refusal decision.

iii Provision of services at the exclusive initiative of the client

A third-country firm will not need any authorisation in Luxembourg in the case of reverse solicitation.

---

10 Article 32(1) of the 1993 Law.

Where a client established or situated in the EU exclusively initiates the provision of investment services by a third-country firm, the requirement for authorisation will not apply to the provision of the investment services by the third-country firm. An initiative by such clients shall, nevertheless, not entitle the third-country firm to market new categories of investment products or investment services to those clients.

III DIGITAL IDENTITY AND ONBOARDING

Regarding digital identity in Luxembourg, the electronic ID (eID) card is a card with an electronic chip that contains digital data and two electronic certificates that allow the holder to authenticate themselves or to sign online documents in various web applications. The eID is issued by the state (i.e., the Government IT Centre (CTIE) – eID applications service). A card reader and a specific application on the user’s computer are needed for use of eID. The reader can be purchased at the CTIE, as well as in certain municipalities. The required software application (middleware) can be downloaded for free on the LuxTrust website. After the application (middleware) is installed and the eID is detected by the card reader, a pin request (secret code) will pop up on the screen. The PIN code must be entered for the first time. After that, the PIN code must be entered at each authentication request from applications being used, or whenever it is needed to sign a document electronically.

The eID is available to Luxembourg nationals only, and not to non-nationals. Non-nationals can, however, use other forms of e-signing techniques (Token, Smartcard, etc.). LuxTrust allows the identification of customers not residing in Luxembourg through a notary and a certificate (apostille) in accordance with international regulations in this area, subject to the production of certain documents (i.e., a copy of the identity card or passport of the person concerned, duly authenticated by a notary).

They can be used by any person of legal age who has requested the activation of the certificates at the time of application for their eID, or by minors of at least 15 years of age for whom the activation of the certificate was requested by either a parent with parental authority or by their legal guardian.

Under certain conditions, the CSSF allows (licensed) financial service providers to identify or verify the identity of their customers through video identification (i.e., the performance of the identification or verification of the identity of the customer by a professional of the financial sector under the supervision of the CSSF (the Professional) through an online videoconference).12

Professionals use this process to support and execute certain tasks for the purpose of fulfilling their customer identification and verification of identity obligations as required by the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended (the 2004 Law).

The Professional has the following possibilities:

- they perform the video identification process themselves using a tool developed internally;
- they perform the video identification process themselves using an external tool acquired from an external provider; or
- they delegate the identification process to an external provider using their own tool.

---

12 CSSF Frequently asked questions on AML/CTF and IT requirements for specific customer on-boarding/KYC methods, version of 8 March 2018.
The video identification needs to be performed by a specifically trained employee, either of the Professional or, if applicable of the external provider.

The video identification or verification of the identity of a customer that is not actually performed by a specifically trained natural person, but where the customer is in contact only with a robot, or where the customer simply uploads (a video with) identity documents online, does not qualify as ‘video identification’ owing to the absence of a live video chat or real-time interaction between the aforementioned trained natural person and the customer.

IV Digital Markets, Payment Services and Funding

The following laws and regulations apply to collective investment schemes:

a. the Luxembourg Law of 17 December 2010 relating to undertakings for collective investment, as amended;
b. the Luxembourg Law of 13 February 2007 relating to specialised investment funds as amended;
c. the Luxembourg Law of 15 June 2004 relating to the Investment company in risk capital as amended;
d. the Luxembourg Law of 12 July 2013 on alternative investment fund managers, as amended;
e. the Luxembourg Law of 23 July 2016 on reserved alternative investment funds;
f. Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse; and

Crowdfunding can be regulated, depending on the platform, but there is no specific licence provided under Luxembourg law.

Whether crowd-lending is permitted depends on how it is structured. If the platform or fintech collects the money before distributing it to borrowers, a licence may be required. Peer-to-peer lending between individuals, however, is not specifically regulated. The role of the platform would then need to be assessed to understand what it actually does. If it is essentially a credit broker that is not linked to a specific credit institution, there is no particular regulation other than the potential need to have a business licence.

With regard to consumer lending regulations, the Consumer Code applies.

The legal restrictions on peer-to-peer lending depend on the terms of the loans, among other items.

For restrictions on trading such loans or financings on a secondary market, see the above text regarding lending professionals.

i Forms of debt securitisation

In specific circumstances, the structures in which the securitisation undertaking itself expressly grants loans instead of acquiring them on the secondary market may be regarded as securitisation, provided that the securitisation undertaking does not allocate the funds raised from the public to a credit activity on own account, and that the documentation relating to the issue either clearly defines the assets on which the service and the repayment of the loans granted by the securitisation undertaking will depend, or clearly describes (1) the borrower
or borrowers; or (2) the criteria according to which the borrowers will be selected, so that the investors are adequately informed of the risks, including the credit risks and the profitability of their investment at the time securities are issued. In both cases, information on the characteristics of the loans granted must be included in the issue documents. The CSSF will assess compliance with these conditions on a case-by-case basis. Moreover, the participants are responsible for ensuring that any other applicable legal provisions are complied with.

ii Impact of the Alternative Investment Fund Managers Law

Pursuant to the CSSF FAQ on Securitisation, according to the clarifications provided by the European Central Bank in its ‘Guidance note on the definitions of financial vehicle corporation’ and ‘securitisation’ under the European Central Bank (ECB) Regulation ECB/2008/30’, point 4.1, page 3, a securitisation vehicle issuing ‘collateralised loan obligations’ would meet the definition of the ECB Regulation, so that these vehicles do not qualify as alternative investment funds.

According to the same Guidance note (points 4.1 and 4.3, pages 3 and 4), securitisation undertakings whose core business is the securitisation of loans that they grant themselves (securitisation undertakings acting as ‘first lender’) do not meet the definition of the ECB Regulation, and thus cannot benefit from the exclusion. The same applies to securitisation undertakings that issue structured products that primarily offer a synthetic exposure to assets other than loans (non-credit-related assets) and where the credit risk transfer is only ancillary.

Payment services require a licence (see Section II.i.2009 Law).

Pursuant to the Payment Services Directive (PSD) II ‘principle of non-discriminatory access to payment systems’, credit institutions are required to open up access to account data to third parties at the request of customers and to support both account information and payment initiation services provided by the third-party payment service providers (TPPs).

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

For the purpose of specific regulation of blockchain technology, on 14 February 2019, a new law was passed by the Luxembourg lawmakers aiming to facilitate the use of distributed ledger technology in financial services. In particular, the law’s main goals are to provide more legal certainty and transparency to the financial market participants, and to allow the use of blockchain technology for the transfer of securities.

Neither CSSF (Luxembourg’s supervisory authority) nor the country’s legislators have come up with any specific legislation related to cryptocurrencies. Thus, there is no legal status of cryptocurrencies yet in place. Nevertheless, both the government and the CSSF

13 CSSF FAQ on Securitisation, What are the various possible forms of debt securitisation?, p.7.
14 AIFM Law means the Luxembourg law of 12 July 2013 on alternative investment fund managers.
16 Loi du 1er mars 2019 portant modification de la loi modifiée du 1er août 2001 concernant la circulation de titres.
are keen to meet with any business intending to operate with cryptocurrencies to discuss the legal possibilities. There are several working groups at the government and CSSF’s level continuously working on new legislation to cater for these business models.

Luxembourg does not cater for a clear statutory definition of ‘securities’, making it difficult to qualify tokens. The term ‘securities’ is viewed as quite general conceptually, and it entails the notions of both ‘valeur mobilière’ and of ‘instrument financier’ (‘transferable security’ and ‘financial instrument’, respectively). Depending on the token characteristics, it may or may not qualify as a security.

Based on Luxembourg legal literature, the term ‘security’ constitutes an application of the materialised rights deriving from a legal act with regard to an issuer and corresponding to specific legal elements that distinguish themselves as being fungible while being allowed to be circulated on the capital markets. Thus, the concept of security approaches more the notion of transferable security, a position that has been also supported by the Luxembourg courts. In general, owing to the broad interpretation of both notions of ‘financial instrument’ and ‘transferable security’ under Luxembourg law, tokens could fall to any of those categories if they are fungible and transferable, and produce cash flow rights or rights to proceeds and returns.

Money laundering rules always apply to cryptocurrencies and tokens. The 5th Anti-Money Laundering Directive also adds ‘providers engaged in exchange services between virtual currencies and fiat currencies’ and ‘custodian wallet providers’ as obliged entities.

In relation to regulated entities in Luxembourg, money laundering rules apply to natural or legal persons trading in goods (only to the extent that payments are made or received in cash in an amount of €10,000 or more, whether the transaction is executed in a single operation or in several operations that appear to be linked). Under these terms, they would fall within the scope of the 2004 Law.

In July 2018, the tax authorities issued a circular clarifying that they treat cryptocurrencies as an asset and not as a currency. The same should, in principle, apply to tokens purchased by a Luxembourg taxpayer. This means that the disposal of cryptocurrencies or tokens (including when used as means of payment) may in certain circumstances give rise to capital gains taxation. These assets will also form part of the net wealth tax base. As regards tokens issued by Luxembourg issuers, their features will be analysed to determine whether the tokens should qualify as debt or equity for Luxembourg tax purposes.

Under Luxembourg law, tokens may be offered to local residents from abroad. However, for such a legal action to be approved, it needs to be subject to Luxembourg consumer protection laws as well as money laundering law restrictions, as the case may be. In addition, if tokens were to be considered as securities, additional requirements would apply.

---


VI OTHER NEW BUSINESS MODELS

Under Luxembourg law, there are not any specific restrictions regarding the use of self-executing contracts. The following elements need to be met in respect of any contract:

- the consent of the party who binds himself or herself;
- his or her ability to sign the contract;
- a specific purpose or object for contracting; and
- a lawful cause.

Arbitration could be agreed upon in a contract (including a self-executing contract) between parties. However, consumers have the right to go to court and any clause prohibiting consumers from going to court would be considered as abusive under the Consumer Code and would be disapplied.

As far as mediation is concerned, a law of 24 February 2012 amended the Luxembourg Code of Civil Procedure to introduce mediation in civil and commercial matters. Any dispute in civil or commercial matters (with certain limited exceptions) may be settled via mediation, which can either be agreed between the parties or ordered by a court. Any contract may include a clause whereby the parties agree to use mediation to settle a dispute. Finally, the CSSF is competent for receiving complaints from customers of the entities subject to its supervision, and to act as an intermediary in order to seek an out-of-court resolution of these complaints.

Subject to specific legal requirements, a fully automated investment process is permitted.

Regarding third-party websites comparing products or providing information about financial products subject to regulation, data protection or competition rules, there is no particular law or regulation in Luxembourg governing comparison websites, and there is no particular definition of this activity. The specific activity of such a website would have to be considered on a case-by-case basis.

If the activity of the website goes beyond the mere comparison of products and disclosure of information and actually provides advice to potential clients, or puts potential clients in contact with credit institutions or professionals of the financial sector and allows them to purchase financial products or services, a licence may be required under the 1993 Law.

Generally speaking, where such a website is addressed to consumers, requirements of the Consumer Code may have to be complied with. In particular, unfair commercial practices, including in particular deceptive commercial practices (e.g., presenting false information) or aggressive commercial practices are prohibited. Assuming the comparison service is offered in exchange for remuneration, it may fall within the scope of the law of 14 August 2000 on electronic commerce, as amended, and specific information requirements may apply. Finally, under the law of 23 December 2016 on, among other things, misleading and comparative advertisement, as amended, misleading advertisement is prohibited.

As far as competition is concerned, the law of 23 October 2011 on competition, as amended:

- imposes the free determination of the price of goods, products and services based on free competition;
- prohibits agreements between undertakings, decisions by associations of undertakings and concerted practices that prevent, restrict or distort competition and in particular, for instance, those which directly or indirectly fix purchase or selling prices; and
- prohibits abuses of dominant position, but does not include specific provisions for this activity.
Finally, to the extent the website offers a service to data subjects in the European Union and processes their data (e.g., by collecting data), Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) would have to be complied with.

Additionally, the law of 13 June 2017 on payment accounts (implementing directive 2014/92/EU) is articulated around three pillars:

a. access to basic payment accounts;
b. bank account switching; and

c. transparency and comparability of payment account fees.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Upon their creation, such business models and related software are automatically protected by copyright.

The company may develop a trademark under which it wishes to sell this product and register such trademark with the European Union Intellectual Property Office.

Once the software is developed, the fintech may also use i-DEPOT operated by the Benelux Office for Intellectual Property (BOIP), as it is a reliable means of proving the existence of an idea at a specific date, before other intellectual property rights, such as trademarks, are acquired.

The fintech will deposit the source code of the program with the BOIP, which keeps the iDEPOT for a period of five to 10 years. However, the iDEPOT does not give rise to an intellectual property right.

Patent protection is not available under the Luxembourg law on patents of 20 July 1992, as amended – software is excluded from patent protection.

Regarding intellectual property rights, unless the provisions of the employment contract are more favourable to the employee, the employer is normally the owner of the developed software or business model. In addition, in principle, no compensation is due.

i Data protection rules

When processing personal data, fintech companies must comply with:

a. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR); and

b. the Luxembourg Law of 1 August 2018 on the organisation of the National Commission for Data Protection and implementing the GDPR.

Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services with the explicit consent of the payment service user.
ii Secrecy rules

2009 Law

The members of the administrative, management and supervisory bodies, directors, employees and the other persons working for payment institutions and electronic money institutions must maintain secrecy of the information entrusted to them in the context of their professional activity. The disclosure of any such information is punishable by the sanctions laid down in Article 458 of the Luxembourg Criminal Code.

There are, however, some exceptions to the professional secrecy requirement, among others, where disclosure of information is required by the law or towards entities in charge of the provision of outsourced services.

1993 Law

Natural and legal persons, subject to prudential supervision of the CSSF pursuant to the 1993 Law or established in Luxembourg and subject to the supervision of the ECB or a foreign supervisory authority for the exercise of an activity referred to in the 1993 Law, as well as members of the management body, the directors, the employees and the other persons who work for these natural and legal persons shall maintain secrecy of the information entrusted to them in the context of their professional activity or their mandate. Disclosure of such information shall be punishable by the penalties laid down in Article 458 of the Criminal Code.

There are, however, some exceptions to the professional secrecy requirement, among others, where disclosure of information is required by the law or towards Luxembourg-based persons subject to the supervision of the CSSF, the ECB, or the CAA, and who are subject to a secret obligation that is criminally sanctioned when the information disclosed to these persons is provided within a service contract.

There are special rules regarding profiling, which are detailed in the GDPR. They mainly concern the following data subject's rights:

a. the right of being informed of the existence of profiling and the consequences of such profiling;

b. the right to object to the processing of his or her personal data for the purposes of direct marketing, including profiling to the extent that it is related to such direct marketing; and

c. the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her that is based solely on automated processing and that produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.

VIII YEAR IN REVIEW

The most relevant developments in the regulation and legal treatment affecting fintechs in Luxembourg are as follows.
The Law of 20 July 2018 implementing PSD II and amending the 2009 Law, which offers equivalent operating conditions to exiting (credit institutions) and new players (TPPs) and submits them to transparency and information requirements.

Changes to the Anti-Money Laundering Directive IV, include:

a
the Law of 13 February 2018, transposing the provisions on the professional obligations and the powers of the supervisory authorities as regards the fight against money laundering and terrorist financing and amending the 2004 Law; and

b
the Law of 13 January 2019, establishing a register of beneficial owners.

The Law of 1 March 2019 on the circulation of securities extends the scope of the Law of 1 August 2001 on the circulation of securities to allow account holders to book and transfer securities through secure electronic recording devices, including distributed electronic registers or databases such as blockchain.

One of the purposes of the AMLD V is to tackle the anonymity of virtual currencies, which may be subject to potential misuse for criminal purposes.

That is why the AMLD V now includes ‘providers engaged in exchange services between virtual currencies’ as well as ‘custodian wallet providers’ in the list of supervised entities subject to AMLD IV requirements.

AMLD V provisions are currently in the process of implementation in Luxembourg (Draft Bill No. 7467 amending the 2004 Law).


22 ‘Virtual currencies’ means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

23 ‘Custodian wallet provider’ means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.
The eIDAS Regulation

The aims of the eIDAS Regulation are:

- to provide a legal framework for secure cross-border electronic transactions; and
- to create an internal market for electronic trust services.

eIDAS Regulation provisions are being currently in the process of implementation in Luxembourg (Draft Bill No. 7427 amending the Luxembourg Law of 14 August 2000 on electronic commerce, as amended).

IX OUTLOOK AND CONCLUSIONS

We expect Luxembourg to continue to attract fintechs and allow them to take advantage of Luxembourg’s highly developed financial ecosystem, and the presence of leading industry players in e-commerce and e-payments, such as PayPal, Amazon and Rakuten or the first EU-licensed crypto-firm, Bitstamp. Luxembourg has also boosted its attractiveness to fintechs by providing a cloud-friendly framework and having the highest density of TIER4 data centres in Europe.

It is to be expected that after the legislator’s recognition of blockchain technology, the next legislative moves will concern tokenisation (whether based on European positions or not) and the structures issuing or using tokens.

---

Chapter 14

MALAYSIA

Shanthi Kandiah¹

I OVERVIEW

It is fair to say that the respective regulators of the financial and capital markets sectors in Malaysia have encouraged fintech developments and, where necessary, proactively adjusted the regulatory framework to facilitate growth. For example, the Malaysian Securities Commission (the SC) was one of the first regulators in the Association of Southeast Asian Nations (ASEAN) region to introduce equity crowdfunding (ECF) guidelines.

There is no specific regulation or special licence for fintech companies in Malaysia. Regulation and licensing requirements are dependent upon the nature of fintech businesses that the company engages in. The Central Bank of Malaysia (the BNM) and the SC are the main regulatory bodies that regulate fintech. The past year has seen the BNM and the SC taking steps to regulate specific areas of fintech, including platform operators and issuers of digital assets, through the issuance of various guidelines and amendments to existing laws and regulations.

There are no tax incentives specifically catering to fintech companies. However, there are tax incentives and preferential tax rates available for certain categories of businesses that could be applicable to fintech start-ups, depending on their business areas. For example, the Malaysia Digital Economy Corporation Sdn Bhd (MDEC) offers a corporate tax exemption for technology start-ups in the Malaysian Digital Hub. At the close of 2019, MDEC announced the government’s approval of the Guidelines on MSC Malaysia Financial Incentives for existing Multimedia Super Corridor (MSC) Malaysia status companies impacted by Malaysia’s participation in the Organisation for Economic Co-operation and Development Base Erosion and Profit Shifting taxation initiatives.

As part of advancing the nation’s digital economy initiative, Finance Minister Mr Lim Guan Eng (as he then was) announced a one-off digital incentive offered by the government to Malaysian citizens. In a move to encourage the adoption of cashless payments in Malaysia, each eligible citizen was entitled to receive a monetary incentive via e-wallet credits through one of three e-wallet operators who partnered with the government under the initiative: Touch ’n Go eWallet, Boost and GrabPay.

¹ Shanthi Kandiah is a partner at SK Chambers. She was assisted in writing this chapter by Thong Xin Lin and Nimraat Kaur.
II  REGULATION

i  Licensing and marketing

A large number of fintech players in Malaysia are involved in the payments and cryptocurrency sectors. A fintech company should always consider in advance whether any licence, approval or registration is required from a regulatory authority, as there is no one-size-fits-all regulation that applies to every fintech player. The regulations that apply will depend on the specific scope of activities of the fintech product or service the company has to offer. Generally, the BNM regulates payment services and currency administration while the SC regulates activities related to capital markets.

The table below captures typical as well as upcoming fintech businesses and their respective regulators and licensing rules, if any.

<table>
<thead>
<tr>
<th>Fintech service</th>
<th>Regulatory body</th>
<th>Licensing/approval/registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-money – a payment instrument that stores funds electronically in exchange of funds paid to the issuer and is able to be used as a means of making payment to any person other than the issuer; it can be issued in different forms such as a digital wallet (e-wallet), which is a type of prepaid account in which a user can store their money for any future online transaction.</td>
<td>The BNM</td>
<td>E-money issuers must obtain approval from the BNM pursuant to Section 11 of the Financial Services Act 2013 (the FSA 2013). According to Division 1, Part 1, Schedule 1 of the FSA 2013, businesses that require approval include those that issue designated payment instruments.</td>
</tr>
<tr>
<td>Merchant acquiring service – a business of an operator of a payment system that enters into a contract with a merchant for the purpose of accepting payment instruments for payment of goods and services.</td>
<td>The BNM</td>
<td>Merchant acquiring services is one of the registered businesses under Schedule 1, Part 2 of the FSA 2013. As such, a person must register with the BNM and comply with the requirements in Section 17 to carry on a merchant acquiring service.</td>
</tr>
<tr>
<td>ECF – enables individuals to invest in a start-up in exchange for shares in that particular company.</td>
<td>The SC</td>
<td>Under the Guidelines on Recognised Markets issued on 17 May 2019 pursuant to the Capital Markets and Services Act 2007 (the CMSA 2007) (the RM Guidelines), an ECF operator must register as a recognised market operator (RMO) with the SC.</td>
</tr>
<tr>
<td>Property crowdfunding (PCF) – a form of fundraising that envisages a homebuyer obtaining funds to pay for the property's purchase price through investments from multiple investors, through an online platform facilitating such transactions.</td>
<td>The SC</td>
<td>Under the RM Guidelines, a PCF operator must register as an RMO with the SC.</td>
</tr>
<tr>
<td>Digital currencies or tokens offered through initial exchange offerings (IEOs) or initial coin offerings (ICOs) – an issuer, typically an early-stage venture, that seeks to raise funds through offering of digital currencies or tokens.</td>
<td>The SC</td>
<td>The Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 (Order 2019) which recognises digital currencies and digital tokens as securities came into force on 15 January 2019. With that, any person who intends to make available, offer for purchase, or issue an invitation to purchase digital currencies or tokens needs to seek authorisation of the SC to do so. Further, an issuer must obtain approval from an IEO operator to offer digital tokens as per the Guidelines on Digital Assets issued on 15 January 2020 pursuant to the CMSA 2007 (the DA Guidelines). An IEO operator refers to an electronic platform operator which is registered pursuant to the DA Guidelines to operate an IEO platform, while IEO refers to offering of digital tokens by an issuer through an electronic platform.</td>
</tr>
<tr>
<td>Peer-to-peer lending (P2P) – a platform enabling individuals to lend money without the use of a bank or a financial institution as an intermediary.</td>
<td>The SC</td>
<td>Under the RM Guidelines, a P2P operator must register as an RMO with the SC.</td>
</tr>
<tr>
<td>Digital asset exchange (DAX) – an electronic platform which facilitates the trading of digital currencies and digital tokens.</td>
<td>The SC</td>
<td>Under the RM Guidelines, a DAX operator must register as an RMO with the SC. Additionally, the trading of any digital asset is subject to the approval of the SC.</td>
</tr>
</tbody>
</table>


## Fintech service

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Regulatory Body</th>
<th>Licensing/Approval/Registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital investment management (DIM) – a company carrying on the business of fund management incorporating technologies into its automated discretionary portfolio management services.</td>
<td>The SC</td>
<td>DIM is a regulated activity pursuant to Part 1, Schedule 2 of the CMSA 2007, and as such must obtain a capital markets services licence from the SC pursuant to Section 58 of the CMSA 2007.</td>
</tr>
<tr>
<td>Digital banking – a banking business or Islamic banking business carried on primarily or wholly through digital or electronic means.</td>
<td>The BNM</td>
<td>Digital banks and Islamic digital banks must apply for a licence with the BNM pursuant to Section 10 of the FSA 2013 or Section 10 of Islamic Financial Services Act 2013 (the IFSA 2013) (whichever applicable). This is subject to the Exposure Draft for Licensing Framework for Digital Banks issued by the BNM on 27 December 2019 being finalised as a policy document and coming into effect.</td>
</tr>
<tr>
<td>Insurance and takaful aggregation business – a business of providing services through any electronic means that: (a) sources, aggregates and compares insurance or takaful products of more than one licensed person; and (b) makes referrals to any such licensed person in respect of the procurement of such insurance or takaful products; or (c) arranges the procurement of such insurance or takaful products through such electronic means.</td>
<td>The BNM</td>
<td>Based on the Exposure Draft for Insurance and Takaful Aggregation Business Registration Procedure and Requirements issued by the BNM on 18 June 2019 (the ITAB Exposure Draft), any persons intending to become a registered insurance and takaful aggregator will be required to be registered under the FSA 2013 to carry on insurance and takaful aggregation business. An amendment to the FSA 2013 is expected to be effected to set out the scope of insurance and takaful aggregation business.</td>
</tr>
</tbody>
</table>

* The DA Guidelines are expected to come into force in the second half of 2020.

### Credit information services

The BNM’s credit bureau, which operates under the Central Bank of Malaysia Act 2009 (the CBA 2009), collects credit-related information on borrowers from lending institutions and supplies the credit information back to the institutions in the form of a credit report via an online system known as the central credit reference information system (CCRIS).

The CCRIS automatically processes the credit-related data received from participating financial institutions and synthesises the information into credit reports, which are made available to the financial institutions and the borrowers, upon request. The credit report contains information on outstanding credit facilities obtained by the borrower, information on credit applications that have been approved in the previous 12 months and pending credit applications made by the borrower.

Subject to approval by the BNM, credit reporting agencies (CRAs) must be registered under the Credit Reporting Agencies Act 2010. There are currently three CRAs that have obtained approval from the BNM, namely Credit Bureau Malaysia Sdn Bhd, CTOS Data Systems Sdn Bhd and RAM Credit Information Sdn Bhd.

### Digital advisory or asset management company

A DIM is a form of fund management regulated under the CMSA 2007. DIM companies providing automated discretionary portfolio management services must obtain a capital markets services licence from the SC pursuant to Section 58 of the CMSA 2007.

Besides the requirements that fund management companies are typically subject to the Guidelines on Compliance Function for Fund Management Companies issued on 14 May 2019 pursuant to the CMSA 2007 (the FMC Guidelines). These impose additional requirements on the DIM itself (e.g., risk management, and algorithm design and oversight) as well as on its board of directors and compliance officer.

In 2018, StashAway Malaysia was the first DIM company to obtain a capital market services licence from the SC to commence operations.
Marketing of fintech products and services

Marketing of fintech products and services depends on whether the fintech company is providing services and products that are regulated in Malaysia. In particular, the following fintech products and services are subject to certain marketing rules:

a Digital assets issued through an IEO – An issuer is required to ensure that all information disseminated for marketing or promotion is consistent with the contents of its White Paper for investors, which is appropriately displayed in all marketing and promotional materials, including its website. An issuer must not engage any third-party individual or entity, other than an IEO operator, to endorse or represent the issuer with the intended purpose of marketing, promoting, gaining publicity or soliciting funds for its digital token offering.

b DIM – Any representations, including in the form of an electronic communication made to clients must be conducted with due care, skill and diligence to enable the clients to make balanced and informed decisions. The DIM company must provide clients with, among other things, adequate information about the DIM company’s shareholding, business address, relevant conditions or restrictions under which its business is conducted, key personnel and persons with whom clients may have contact, and subsequent changes made thereafter. Any advertisements or promotional materials issued by a DIM company must be fair, accurate and timely and must include specific matters identified under the FMC Guidelines, including risk of investments and any conflict of interest that may arise from investments.

ii Cross-border issues

Regulated or licensed activities cannot be passported from another jurisdiction into Malaysia. Fintech companies licensed in a foreign jurisdiction that intend to offer their services or products in Malaysia must obtain the relevant licences and approvals under the applicable Malaysian laws.

Presently, all ECF, P2P, DAX, PCF and IEO operators are required to be locally incorporated. There are also additional requirements for issuers on ECF, P2P and IEO platforms to be locally incorporated. Besides the requirement for issuers on IEO platforms to be locally incorporated, the issuer must also carry out its main business operations in Malaysia and its board of directors must include at least two directors whose principal or only place of residence is in Malaysia.

Malaysia has a liberal foreign exchange policy whose rules apply depending on residency status. Non-resident investors are free to undertake any type of investment in ringgit assets or foreign currency assets in Malaysia (direct or portfolio investment) without any restriction, and to repatriate divestment proceeds, profits, dividends or any income arising from investments in Malaysia. Similarly, residents without domestic ringgit borrowing are free to invest in foreign currency assets onshore and abroad.

III DIGITAL IDENTITY AND ONBOARDING

In 2001, it was made compulsory for all Malaysians to hold a national identity card known as ‘MyKad’, which contains an individual’s name, address, race, citizenship status, religion and an inbuilt chip that stores fingerprint biometric data. The MyKad is primarily used as an official identification document to verify an individual’s identity and can also be used as an ATM card, an e-wallet and a transit card.
The MyKad also enables Malaysians to access MyEG – an electronic government (e-government) service platform – that provides an array of government services such as renewal of foreign workers’ permits, replacement of national identity cards, payment of parking summons, car insurance and road tax renewals, and temporary transfers of vehicle ownership. The e-government services are also available to companies. A representative of a company would be required to provide their MyKad as a verification tool in order to access the e-government services.

As the MyKad is a physical identification document used to verify a person’s identification, it does not qualify as a digital identity. In August 2019, the Minister for Communications and Multimedia (the Minister) announced the Cabinet’s approval of the implementation of the National Digital Identity initiative. According to the Minister, although the National Digital Identity is an advanced method of authenticating a user’s identity online, it does not substitute the MyKad, nor will it be made compulsory.

The Minister further added that the Malaysian Communications and Multimedia Commission (MCMC) will conduct a detailed nine-month study to identify a holistic National Digital Identity framework, which will include recommendations to the government on appropriate implementation models, taking into account the existing MyKad and private infrastructure, among other factors. The MCMC commenced this comprehensive study to establish a user-centric National Digital Identity framework for Malaysians on 21 November 2019, and will be working with relevant stakeholders to gather their views on potential use cases for the National Digital Identity platform. The study will include local contextual analysis, implementation strategy, operating model, technology and enabling policies as well as related legislations.

When proposing the National Digital Identity in October 2018, the Minister stated that the scheme aimed to provide a ‘verifiable platform of trust’ to reduce the possibility of fraud, which is common in e-commerce transactions. The National Digital Identity will provide a platform to verify the identity of an individual, thus reducing the scope of such crimes.

As the framework is still being formulated, it is not known whether it will extend to fintech businesses and non-residents of Malaysia.

Digitised onboarding is a relatively new process in the financial services sector. Efforts to introduce digitised onboarding in the financial services sector in Malaysia are highlighted by the BNM issuing the Exposure Draft for Electronic Know-Your-Customer (e-KYC) on 16 December 2019 (e-KYC Exposure Draft). The e-KYC Exposure Draft sets out proposed requirements and guidance in implementing e-KYC solutions for the onboarding of individuals to the financial sector and the proposed requirements outlined in the exposure draft are aimed at enabling safe and secure application of e-KYC technology in the financial sector, facilitating the BNM’s continued ability to carry out effective supervisory oversight over financial institutions, and ensuring effective anti-money laundering and counter financing of terrorism (AML/CFT) control measures are in place.

In 2017, CIMB Bank Berhad was the first Malaysian bank to receive the BNM’s regulatory sandbox approval to implement the e-KYC method for customer-identity verification. In implementing e-KYC, financial service providers may be subject to the Personal Data Protection Act 2010 (the PDPA 2010), which sets out the seven data protection principles including the general principle establishing the legal requirements for processing data, notice, choice, disclosure, data security, integrity and retention, and rights of access.
IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

As stated in Section II, the regulations that apply will depend on the specific scope of activities of the fintech product or service the company has to offer. The relevant licence, approval or regulations required for the relevant fintech product or service is set out in Section II above.

The SC, which regulates activities related to capital markets appears to also be regulating specific areas of fintech relating to ECF, P2P, PCF and DAX pursuant to the CMSA 2007. These respective areas of fintech are also subject to additional requirements as set out in the RM Guidelines. For ECF and P2P financing, the RM Guidelines impose additional requirements on platform operators (e.g., operation of trust account, obligations and managing conflict of interest) and the issuer (e.g., limit to funds raised on platform and disclosure requirement). Investors may also be subject to a restriction on investment amounts, depending on the status of the investor. Additional requirements relating to a PCF platform would mainly be imposed on the platform operator (e.g., criteria to qualify, prohibition on financial assistance, obligations, exit certainty, eligibility and obligations of homebuyers, disclosure requirements, client’s asset protection), although homebuyers would also be subject to certain restrictions on the amount of funds permitted to be raised through a PCF platform, and only a property that satisfies the criteria prescribed under the RM Guidelines is eligible to be hosted on a PCF platform. Among other things, DAX operators are prohibited from providing financial assistance to investors to invest or trade in digital assets on its platform.

On the other hand, the BNM regulates payment systems and currency administration, and, therefore, the operation of a payment system and the issuance of a designated payment instrument requires the approval of the BNM pursuant to the FSA 2013.

Collective investment schemes, which consists of unit trusts, real estate investment trusts, exchange-traded funds, closed-end funds, sustainable and responsible investment funds, foreign collective investment schemes and ASEAN collective investment schemes, are presently governed by the SC. It appears that fintech schemes presently do not fall within the scope of collective investment schemes although certain fintech products and services are regulated pursuant to the CMSA 2007.

The RM Guidelines allow for trading of investment notes and Islamic investment notes on a PCF platform provided that such investment note has been hosted and successfully funded through the PCF platform. In this regard, a PCF operator would be required to comply with the relevant requirements in the RM Guidelines (e.g., disclosure of information; adequate arrangements to deter market manipulation, manage error trades; manage systems error, failure or malfunction; make available pre-trade and post-trade information on non-discriminatory basis to all users on a timely basis).

Any disclosure of client data or product data to third parties is subject to the PDPA 2010.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

Order 2019 recognises digital currencies and tokens as securities and would therefore be subject to applicable securities law (i.e., the CMSA 2007). Any person who offers or issues an invitation to purchase digital currencies or tokens will need to seek authorisation of the SC to do so.
Digital tokens are regulated as securities where they represent a right or interest of a person in any arrangement made for the purpose of, or having the effect of, providing facilities for the person where:

- the person receives the digital token in exchange for a consideration;
- the consideration or contribution from the person, and the income or returns, are pooled;
- the income or returns of the arrangement are generated from the acquisition, holding, management or disposal of any property or assets or business activities;
- the person expects a return in any form from the trading, conversion or redemption of the digital token or the appreciation in value of the digital token;
- the person does not have day-to-day control over the management of the property, assets or business of the arrangement; and
- the digital token is not issued or guaranteed by any government body or central bank as may be specified by the SC.

On 15 January 2020, the SC further issued the DA Guidelines, which outline the framework for fundraising through digital token offerings in Malaysia. The DA Guidelines set out requirements for an issuer to carry out all digital token offerings through an IEO operator registered with the SC. An issuer must be a company incorporated in Malaysia and carry out its main business operations in Malaysia. The issuer’s board of directors must have at least two directors whose principal or only place of residence is in Malaysia. It is pertinent to note that an issuer must not be hosted concurrently on multiple IEO platforms or on an ECF platform.

Additionally, the IEO operator must also be a locally incorporated company and is required to carry out the necessary assessment and due diligence to verify the business of the issuer as well as to understand the features of the digital tokens that are to be issued. In the event that the IEO operator wishes to facilitate the trading of digital assets on its platform, the IEO operator must also register with the SC as a DAX operator.

The DA Guidelines also emphasise that if a digital token serves as a payment instrument, the digital token may only be used in exchange for the issuer’s goods and services disclosed in the issuer’s White Paper, which is approved by the IEO operator.

Separately, the RM Guidelines were also amended to include the requirements for DAX operators to be registered as RMOs. DAX operators who are not approved by the SC are required to cease all activities immediately and return all monies and assets collected from investors.

Amendments made to the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the AMLA 2001), which came into effect on 2 January 2018, sought to extend the scope of a reporting institution to include any person who carries out activities that provide services in relation to the exchange of digital currencies. The reporting obligations pursuant to the AMLA 2001 include keeping a record of or promptly reporting to the competent authority any transaction involving the domestic currency or any foreign currency exceeding such amount as the competent authority may specify. The BNM also issued the Anti-Money Laundering and Counter Financing of Terrorism – Digital Currencies (Sector 6), which came into effect on 27 February 2018 (the Sector 6 Policy Document). The Sector 6 Policy Document sets out minimum requirements and standards that a reporting institution must observe to increase the transparency of activities relating to digital currencies including in relation to risk assessment and customer due diligence.

© 2020 Law Business Research Ltd
It remains to be determined if cryptocurrencies are subject to tax law, as there is no specific provision for digital currency in the Income Tax Act 1967. However, Malaysia's Inland Revenue Board (IRB) appears to be paying more attention to the tax position of cryptocurrencies. In an update release dated 12 January 2018 by Luno, a London-based digital exchange, the IRB temporarily froze the bank account of Bitx Malaysia, Luno's local entity in Malaysia. The bank account was frozen pending tax investigations. In an update release dated 2 February 2018, Luno stated that the IRB had agreed to unfreeze the bank account while in the process of completing the investigation.

VI  OTHER NEW BUSINESS MODELS

There is no specific law governing the use of self-executing contracts (smart contracts) in Malaysia. However, these contracts would need to adhere to the general principles of creating a legally valid contract, including offer and acceptance, consideration and intention to create a legal relationship. The increased number of fintech companies that offer smart contract development services demonstrates the increasing demand for smart contracts in Malaysia, which may affect the need to regulate smart contracts in Malaysia.

The Electronic Commerce Act 2006 (the ECA 2006) recognises the validity of a contract that is formed wholly or partly in electronic form. Communication of proposals and acceptance of proposals in the form of electronic messages is recognised as a valid and enforceable contract. Furthermore, the ECA 2006 provides that the Digital Signature Act 1997 (the DSA 1997) applies to any digital signature used as an electronic signature in any commercial transaction. The DSA 1997 states that where a document is signed with a digital signature it shall be as legally binding as a document signed with a handwritten signature, an affixed thumbprint or any other mark.

Third-party websites comparing or providing information about financial products are not regulated per se. However, the BNM recently issued the ITAB Exposure Draft whereby, upon coming into effect, any person carrying out such business must register with the BNM pursuant to the FSA 2013. Activities of price-comparison sites would also be subject to existing laws, such as the Competition Act 2010 (the CA 2010) and the PDPA 2010. The main prohibitions against anticompetitive agreements or abuse of dominance would govern the activities of price-comparison sites. In other words, cases actioned in other jurisdictions as being anticompetitive or potentially so can be actioned under the provisions of the CA 2010. For example, where:

\[a\] price-comparison sites have been found to facilitate information exchange between competitors; or

\[b\] the use of most-favoured-nation clauses leads to one comparison site always having the best deals, making it harder for other sites to effectively compete in the market, thus leading to the foreclosure of these other sites from the market.

Intellectual property and personal data protection considerations are further discussed in Section VII.

Artificial intelligence (AI) has made headway in the local banking sector in the form of chatbots. RHB Bank Berhad launched an AI-powered messenger platform that operates in real time to streamline the credit card application process. Hong Leong Bank Berhad and the
CIMB Group have also launched virtual assistants by employing AI technology. Presently, there are no special rules applicable to the use of AI in financial products as imposed by the BNM. However, businesses modelled based on AI would still be subject to existing laws.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Fintech business models and related software can be protected by various intellectual property rights, namely copyright and patent. Alternatively, protection as confidential information under common law in Malaysia is also available, depending on the nature of the business model. Software is generally protected by copyright under the Copyright Act 1987, with no requirements for registration.

Patent protection is available for new inventive steps involving industrially applicable products and processes. In short, it provides a wider range of protection than copyright as it protects the idea or concept rather than just the work (e.g., source codes for software) – hence, business models would likely gain patent protection by filing a patent application.

If an employee develops an original work during his or her term of employment, the default rule is that ownership of the copyright vests in the employer. Alternatively, if a contractor develops an original work, the default rule is that the contractor continues to own the original work. However, it is common for employees and contractors to be bound by written contractual obligations that specify ownership of the intellectual property they develop, and these default rules may be overridden. Compensation, if any, owed to the author of the copyright work would also depend on the nature of the relationship or the agreements entered into between the parties. Fintech companies should ensure that their employees and contractors enter into agreements specifying the rules on ownership of intellectual property.

The PDPA 2010 would also apply to fintech companies if they process any personal data (e.g., client data). Apart from the seven principles set out in the PDPA 2010, there are no rules that apply specifically to the digital profiling of clients. A data subject must consent to the processing of the personal data unless the processing is necessary for specific exempted purposes. Although the PDPA 2010 does not define or prescribe any formalities in terms of consent, the Personal Data Protection Regulations 2013 provide that the data user must keep a record of consent from data subjects and that the Personal Data Protection Commissioner or an inspection officer may request this.

There is no system of registration for confidential information. Business models and software can be protected if they are confidential in nature, disclosed in circumstances imposing confidentiality and there is actual or anticipated unauthorised use or disclosure of the information.

In addition, financial institutions in Malaysia are subject to secrecy rules in relation to customer affairs or account information as per Section 133 of the FSA 2013.

VIII YEAR IN REVIEW

The following highlights the SC and BNM initiatives in the regulation of fintech services in Malaysia.

The recognition of digital currencies and tokens as securities through Order 2019 has paved the way for the regulation of cryptocurrencies in Malaysia and has introduced some level of certainty as to the permissibility of offering and trading digital currencies and tokens. It is worth noting, however, that the coming into effect of Order 2019 and amendments...
made to the RM Guidelines to introduce requirements for DAX operators has resulted in a sharp decline in the number of DAX operators in the market, as currently there are only three DAX operators registered as RMOs with the SC, namely Luno Malaysia Sdn Bhd, Sinegy Technologies (M) Sdn Bhd and Tokenize Technology (M) Sdn Bhd.

Following the government’s initiative to provide an alternative financing avenue for first-time home buyers, the SC released a PCF framework. This is pursuant to the amendments made to the RM Guidelines issued on 17 May 2019 setting out a new chapter on additional requirements applicable to a PCF operator. On 25 September 2019, EdgeProp Sdn Bhd became the first PCF operator registered as an RMO with the SC. The SC also announced eight new RMOs consisting of three ECF operators and five P2P operators in 2019. To date, there are 21 ECF and P2P operators registered as RMOs with the SC.

In line with the BNM’s efforts to support the development of technology-based innovations in the financial sector, the BNM issued the Exposure Draft on Licensing Framework for Digital Banks on 27 December 2019. The Exposure Draft outlines the proposed framework for entry of digital banks with innovative business models seeking to offer banking products and services to address market gaps in the underserved and unserved segments. The BNM will be issuing up to five licences to qualified applicants to establish digital banks to conduct either conventional or Islamic banking business in Malaysia. Digital banks will also be required to comply with the requirements under the FSA 2013 or the IFSA 2013, whichever is applicable, including relevant requirements relating to standards on prudential, business conduct and AML/CFT. The BNM aims to finalise the policy document by the first half of 2020.

IX OUTLOOK AND CONCLUSIONS

The advent of fintech has brought about the need for regulation in the fintech industry. The approach taken by the BNM and the SC suggests that fintech is welcomed, although regulation for the sector is still necessary. While regulations have started to be introduced in a number of areas in fintech, it remains to be seen how these regulations will be enforced, especially after the DA Guidelines come into effect.

With ECF, P2P and PCF platforms coming into play, as well as the growing popularity of DIM services, Malaysians now have the opportunity to diversify their investment portfolios. The guidelines and regulations of these platforms by the SC minimise investment risks and create a more reliable environment for Malaysians to invest their money.

There is also great anticipation for the second half of 2020 once the Digital Banks Exposure Draft has been finalised as a policy document and comes into effect. It is expected that this will encourage the foray of non-banking players into the banking industry.
I OVERVIEW

The Law to Regulate Financial Technology Companies (the Fintech Law), and secondary regulations were enacted over the past few years in Mexico. All secondary regulations had to be enacted no later than March 2020, although certain regulations remain pending.

Regulated fintech entities, which are considered part of the financial services sector, are mainly regulated by four governmental agencies:

a) the Bank of Mexico (Banxico) as the Mexican central bank;

b) the Ministry of Finance and Public Credit (SHCP) as the ministry within the executive branch in charge of regulating financial institutions;

c) the National Banking and Securities Commission (CNBV) as an agency that directly depends on the SHCP; and

d) the Financial Consumer Protection Commission (CONDUSEF).

Notwithstanding the above, the National Insurance and Bonds Commission (CNSF) and the National Retirement Savings System Commission (CONSAR) are also authorised under the Fintech Law to perform certain surveillance activities.

While it is true that the spirit of the Fintech Law is to permit fintech companies to do business in Mexico, secondary regulation is very exhaustive which may have resulted in an overregulation. In our opinion, depending largely on how the regulations are applied and enforced, Mexico could become a fintech-friendly jurisdiction but with clear oversight by financial regulators.

Although regulated fintech entities are part of the financial sector, they are not part of the financial system for tax purposes, and therefore have the same rights and obligations as any other entity incorporated pursuant to Mexican law.

This chapter describes the Fintech Law and the main principles and guidelines therein to regulate fintech companies.

II REGULATION

i Licensing and marketing

The Fintech Law mainly seeks to regulate two kinds of fintech companies: crowdfunding companies and e-money companies.
Crowdfunding companies are defined as the technological platforms that connect people so that investors can fund investment seekers through mobile applications, interfaces, websites or any other means of electronic or digital communications. Their activities are described further below. E-money companies are those entities that may provide issuance, administration, redemption and transmission of e-money. Both companies may operate with cryptocurrencies, which in accordance with the law are called ‘virtual assets’.

A special licence is required to operate as a crowdfunding or an e-money company, issued at the discretion of the CNBV prior to approval of the Inter-institutional Committee, which comprises two members of the Ministry of Finance and Public Credit, two members of the CNBV and two members of Banxico.

In general terms, entities interested in obtaining a licence to act as a fintech company shall be incorporated as corporations, setting forth in their corporate by-laws that:

a. their purpose is to engage in any of the fintech activities described in the Fintech Law (crowdfunding or e-money);

b. they are subject to the provisions set forth in the Fintech Law and relevant secondary regulation;

c. they designate a domicile within Mexico; and

d. they have a minimum amount of capital, in accordance with their activities, as defined by the CNBV through secondary regulation.

The minimum capital depends on the activities that fintech companies will perform and the risk that they will assume. Crowdfunding entities that perform only one type of activity (debt, capital or co-ownership funding) must have a minimum capital of 500,000 investment units2 (currently this is around 3.2 million Mexican pesos) this minimum capital is also applicable to e-money companies that perform their activities in national currency. Crowdfunding entities that are authorised to perform two or more activities and e-money companies that are authorised to perform their activities in foreign currency or with virtual assets or that are authorised to perform underlying virtual assets derivative transactions or act as a switch, shall have a minimum capital of 700,000 UDIs (currently this is around 4.5 million Mexican pesos).

Applicants shall also provide:

a. the power of attorney granted, before a notary public, to the legal representatives to submit for application the request to be considered a fintech company;

b. a draft of corporate by-laws that comply with the requirements set forth above and others contemplated in the Fintech Law;

c. a business plan;

d. segregated accounts as provided in the Fintech Law;

e. the means and policies to comply with risk disclosure;

f. means and policies implemented regarding operational risks, confidentiality and evidence of having a technological support for their clients, and compliance with the minimum security standards against fraud or cyberattacks;

g. operational controls and processes for client identification;

h. conflict-check policies;

i. AML, fraud prevention and non-terrorism finance policies;

j. agreements with other fintech companies for the performance of key business processes;

---

2 As at 17 March 2020, 1 investment unit (UDI) is equivalent to 6.492514 Mexican pesos.
k a list of the persons that, directly or indirectly, hold or intend to hold an equity participation (describing the amount of their participation and the origin of the resources);

l a list of the board members of the company including their background and credit report;

m information required to verify the ownership or right of use of the interface, website or electronic means of communication;

n domicile within Mexico and a legal representative;

o information related to incentives (only applicable to crowdfunding companies); and

p other documents required by CNBV in secondary regulations.

The requirements requested above are designed to comply with the principles of the Fintech Law, and specifically to principles related to financial stability and fraud prevention.

The Fintech Law is close to a disclosure-based regulation. Therefore, fintech companies are required to implement measures to avoid spreading false or misleading information to comply with the principle of consumer protection. Additionally, fintech companies shall inform their clients about the risks of transactions executed through them. Specifically, they need to make it clear on their websites, applications, contracts and electronic or digital communications, and marketing adverts that neither the federal government nor the entities managed by the public state-owned administration support or back their obligations and that there is no deposit insurance, but that they are authorised, regulated and supervised by Mexican financial authorities. Additionally, their corporate name must indicate whether they are crowdfunding or e-money companies.

The Fintech Law does not regulate the activity of automated-digital advisory services or asset management. However, advisory services may be carried out with a prior registration with financial authorities. Investment advisers are regulated for AML and consumer-protection purposes but their regulation is probably lighter than the regulation that will apply to fintech companies. Automated asset management may be provided through an investment adviser as long as he or she operates through a licensed broker-dealer and is not the custodian of the assets.

Considering the provisions set forth within the Fintech Law, sharing of information is subject to secondary rules issued by the Supervising Commission and Banxico. In this sense, the Fintech Law provides that financial entities, money transmitters, credit-scoring companies, clearing houses, fintech companies and companies authorised to operate with innovative models will be required to establish programming interfaces of standardised applications that allow connectivity and access to other interfaces developed or managed by them and the allowed IT third parties, to share the following information:

a open financial information, which is defined as that information generated by the above-mentioned entities that is not confidential. In other words, open financial information may be referred to those related to the product or services offered to the general public and the location of its offices, ATMs and other points of service on which its products or services may be accessed;

b aggregated data, which is defined as statistical information that does not identify an individual and that is related to operations made by or through the entities mentioned above; and
transactional data, which is defined as information related to the use of a product or service, including deposit accounts, credit and means of disposition contracted on behalf of clients, and other information related to transactions that customers have made or tried to perform in the technological infrastructure of the above-mentioned entities.

Access to open financial information is not limited by the Fintech Law. Regarding aggregated data, the Fintech Law provides that access will be limited to those persons that have implemented authentication methods, as provided by the supervising regulators, Banxico or the credit-scoring companies through the provisions within the secondary regulations issued to that end and, finally, transactional data shall be shared with the client’s consent only and shall be used for the purposes expressly consented to by the client.

ii Cross-border issues

There is no limitation within the Fintech Law for Mexican-licensed fintech companies to offer their services abroad.

There is also no limitation on foreign ownership of Mexican fintech companies. They may be wholly owned by foreigners or foreign investors. Neither are there exchange or currency control restrictions. Foreign companies should consider, however, that as general rule, any person in Mexico has the right to settle his or her obligations payable within the Mexican territory in Mexican pesos at the official exchange rate published by Banxico.

On the other hand, foreign fintech companies may not offer or market their services in Mexico without a local licence. The Fintech Law does not address how it applies to companies that have no physical presence in Mexico, but if a fintech company is intentionally and regularly marketing to Mexican customers the financial regulators are likely to try asserting jurisdiction and applying the Fintech Law and Mexican regulations, as with any other financial entity doing business in Mexico without a physical presence. What 'regularly' means is something that is yet to be tested and will need to be analysed on a case-by-case basis.

III DIGITAL IDENTITY AND ONBOARDING

Currently there is no recognised digital identity in Mexico. The prior federal administration had plans to implement a digital nation on which technology and innovation converged to reach the goals for the development of the country, and the implementation of a digital identity. However, the current federal administration has not issued any statement as to whether it will continue with the previous digital national strategy or whether it will have its own strategy. Many Mexican citizens still lack access to diverse services (including financial services) by using a digital identity.

Up to now, some governmental entities have digital databases based in biometrical systems and have created through them a kind of digital identity for some Mexican citizens and foreign residents; biometrical systems are the core required for the implementation of a digital identity in Mexico, but are not generally adopted yet by all entities.

Private means of creating a digital identity are not prohibited by the Mexican authorities but there is still no general system available that may function as a digital identity. Banks will be obliged as of March 2020 to request biometrical data (i.e., fingerprints) of their clients to verify their identity when requesting a loan or opening an account. The biometrical information collected by the banks will be matched with the database of the National
Electoral Institute (or with the National Immigration Institute, in case of foreigners) to verify customers’ identity. Banks have agreed to use a sole database that may be supplemented by the databases of other governmental entities such as the tax administration database. A bank’s database, when implemented, may be considered an initial, but a private and limited digital identity database.

There is no provision related to mechanisms that may be implemented by fintech companies regarding the use of a digital identity; nevertheless, such companies are implementing diverse private methods to verify its users’ identity. Means used by fintech companies may vary and contain different requirements related to the documents or validation of proofs requested by the relevant users. As mentioned before, identification methods may vary but the most common means used by fintech companies are currently:

- **a** online validation of a mobile number;
- **b** ID validation (by taking a picture of the relevant user in conjunction with his or her ID);
- **c** valid proof of address;
- **d** linking a fintech account to a bank account in order to receive or transfer funds; and
- **e** physically or electronically sign a written agreement.

Crowdfunding companies and e-money companies are required to implement identity checks through the completion of a know-your-customer procedure. For these purposes, crowdfunding companies and e-money companies must obtain from their customers information and documents, which will vary depending on whether their customer is a foreign or national individual, foreign or national entity or other, as provided under the secondary regulation issued by the CNBV and the entity’s anti-money laundering manual.

The information and documents that must be collected from customers can be collected remotely through automated questionnaires and digital copies of the documents.

Pursuant to the relevant secondary regulation, fintech entities shall file reports with the CNBV for, among others, any relevant or unusual operation performed by their customers, as well as transactions performed with foreign currency or virtual assets.

### IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

The Fintech Law regulates crowdfunding and expressly allows for different models such as peer-to-peer lending and collective investment schemes. Crowdfunding companies may operate debt investment schemes, equity investment schemes, co-ownership and royalty investment schemes.

The Fintech Law does not allow crowdfunding entities to securitise or trade loans in secondary markets. Furthermore, the Fintech Law provides that crowdfunding companies cannot take loans or issue securities whenever those loans or securities are issued to ‘share risks’ with investors.

As mentioned before, crowdfunding and e-money companies need a licence that will be granted at the discretion of the CNBV, prior to the approval of the Inter-institutional Committee.

Licensed crowdfunding companies may only engage in the following activities:

- **a** receive and publish the requests of crowdfunding operations of borrowers or targets and their projects through its interface, website or electronic or digital communication means used to perform its activities;
Mexico

b provide information to the potential investors so that they know the characteristics of the requests of crowdfunding or projects;

c enable and allow electronic means of communications between investors and borrowers;

d obtain loans and credits;

e issue securities;

f own or lease real property;

g make deposits in authorised financial companies;

h create a trust required to comply with their legal purpose (e.g., to segregate funds);

i make investments in complementary, auxiliary or real estate companies;

j perform judicial or extrajudicial collection of credits granted to borrowers by investors, as to renegotiate the terms and conditions of relevant credits; and

k other activities required to comply with their corporate purpose.

E-money companies are only allowed to engage in the following activities:

a issue, commercialise or manage instruments for the disposal of funds of electronic payments;

b provide the service of money transmission;

c provide services related to payment networks;

d process information related to payment services;

e grant credits or loans only as overdrafts of the accounts they administer;

f operate with cryptocurrencies;

h obtain loans and credits of any local or foreign person in order to comply with their corporate purpose;

i constitute overnight or term deposits in financial institutions;

j own or lease real property;

k broker with cryptocurrencies; and

l buy, sell or transfer cryptocurrencies on their own account.

As mentioned above, sharing information rules are subject to secondary regulations issued by the Supervising Commission and Banxico. The Fintech Law provides that fintech companies (among the other entities mentioned within the law) will be obligated to execute an agreement with transferees and set forth therein that they (transferees) will be required to allow audits by fintech companies to verify compliance with the Fintech Law. Fintech companies will be required to report the results obtained of such audits to the Supervising Commission and Banxico.

The CNBV is the authority in charge of issuing general provisions related to information security, which include confidentiality policies and registry of accounts related to transactional movements, the use of private or public technological means or other systems for processing of information that will apply to crowdfunding companies. In the case of e-money companies, the foregoing provisions are issued by the CNBV in conjunction with Banxico.

Fintech companies are required to retain information in a physical or electronic format for minimum terms of 10 years.
V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

Cryptocurrencies are known as virtual assets in the Fintech Law and they are defined as a representation of value, electronically registered and used by the public as a means of payment for any legal transaction and transfer of which may be made only through electronic means. In accordance with the Fintech Law, cryptocurrencies may not be considered legal currencies, and licensed fintech companies may operate only with such cryptocurrencies previously approved by Banxico. Fintech companies require a special authorisation from Banxico to operate with cryptocurrencies. Banxico issued Circular 4/2019, which provides that fintech entities will not be authorised to operate if their purpose is to exchange, transfer or safeguard cryptocurrencies. Currently, fintech entities and financial institutions will only be permitted to trade with cryptocurrencies on their own account (proprietary trading).

No specific technology is regulated by the Fintech Law or its secondary regulation. Blockchain technology is not regulated by the Fintech Law or by any other Mexican laws. The Fintech Law regulates activities and transaction and, generally, does not speak of specific technologies.

VI OTHER NEW BUSINESS MODELS

The Fintech Law devotes a special chapter to innovative models, which are defined as ‘those that to provide fintech services employ tools or technological means with alternatives different from those currently existing in the market’. As mentioned in this chapter, the Fintech Law is designed as a principle-based regulation and, in keeping with this, such chapter is in line with principles of innovation and promotion of competition, by opening its text to admit new models of services and the admittance to new competitors to the fintech environment.

Innovative models will receive a temporary authorisation that will be discretionally granted by the financial authorities when the applicant duly proves that:

a it has an innovative model;
b the product or service to be offered to the public shall be tested in a controlled environment;
c the new model represents a benefit to the client that cannot be obtained from existing models available in the market;
d operations may be made immediately;
e the project shall be tested with a limited number of clients; and
f other requirements that are to be determined by financial authorities.

Temporary authorisation may not be granted for longer than two years and shall be in accordance with the services that will be or are planned to be provided.

Authorisation shall be requested from the competent authority depending on the purpose of the innovative models, this meaning that either CONDUSEF, CONSAR, CNSF, the CNBV, Banxico, or two or more of these authorities may empowered to review the innovative model. Financial authorities may authorise fintech companies, financial entities or others to implement and operate innovative models.

All entities authorised to operate an innovative model shall have: (1) the human, monetary and material resources to operate their model during the term of the authorisation;
(2) policies in place to mitigate the risks to which customers will be exposed; and (3) the resources, insurance or other types of guarantee to indemnify their customers for any damages and lost profit caused during the temporary authorisation.

Entities authorised to operate innovative models shall give the competent financial authority a quarterly report containing the number of transactions performed during such term, the number of clients, the risk factors generated during the applicable term and the actions taken to secure a final authorisation.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

In Mexico, software is not subject to be patented. The Industrial Property Law specifically provides in its Article 19(IV) that software may not be considered as an invention. In practice, software is registered as an intellectual work in accordance with the provisions set forth in the Federal Copyright Law. The foregoing provisions apply to fintech business models and related software; in both cases, they may be registered under the copyright provisions.

Considering the above, in accordance with the provisions set forth within the Federal Copyright Law, when an individual or company requests a contractor to develop software or business models, by the payment of remuneration, the company will own the economic rights over the work and have the rights related to its divulgation, integrity and collection.

Regarding contractors, they may have the right to be expressly mentioned in the role of authors over the parts in which they have participated. It is essential that agreements are drafted in a clear manner and that the terms of the work to be created and its remuneration are stated precisely, considering that in case of doubt, interpretation will be in favour of the author.

When a work is made as a consequence of a labour relationship, established within a written individual labour agreement, it will be presumed, if it is not otherwise agreed, that economic rights will be divided equally between employer and employee. The employer may divulgate the work without the authorisation of the employee but not the other way around. If an individual labour agreement is absent, economic rights will be granted to the employee.

Regarding privacy rights, the Fintech Law regulates the exchange of information with authorities. Specifically, it provides that fintech companies are required to provide information to the CNBV and Banxico about their operations and their clients, including data that may be useful to estimate their financial situation and information that may be useful for mentioned authorities in order to duly comply with their functions.

Additionally, the Fintech Law provides that clients’ information shall be considered as confidential and that in no case may fintech companies give notices or information of their activities or services contracted by them unless such information is requested by the client itself, his or her legal representatives or those whose have granted a power of attorney to intervene in the relevant operation or service. This is similar to current banking secrecy provisions.

There are no special rules applying to the digital profiling of clients considering that processing of personal data is not distinguished if physical or electronic means are implemented for this purpose. On this topic, the Federal Law on the Protection of Personal Data held by Private Parties (the Data Protection Law), requires data controllers to obtain consent before processing data subjects’ personal information and to obtain that consent through the delivery of a detailed privacy notice that contains at least the requirements set
forth within the privacy law framework applicable within Mexico. Furthermore, financial information shall be protected under stricter means and measures than identification data. When processing financial information, express consent is required.

The Data Protection Law also requires data controllers to process personal information in accordance with the following principles: lawful basis for processing; consent; information; data quality; purpose limitation; loyalty; proportionality; and responsibility.

Data controllers shall also adopt the security measures and procedures that are necessary to protect the personal data against damage, loss, alteration, destruction and unauthorised use, access or processing. These measures shall be at least equal to the measures that the data controller uses to protect the company’s own information.

If storage is through a cloud computing service provider, the storage will be subject to specific conditions provided within the Regulations of the Data Protection Law. The data controller and service provider (i.e., the cloud computing service provider) relationship, shall be documented within a legal instrument and the relevant service provider, in its role of data processor, shall be informed about the data controller’s (company) privacy notice and may only process the personal data received by the data controller, in accordance with its privacy notice and its instructions.

The data controller shall only contract services from a provider that it:

- has policies and procedures similar to those contemplated by the Data Protection Law and the Data Protection Regulations;
- discloses if it subcontracts to third parties;
- does not condition the service upon the service provider becoming the owner or acquiring any right over the personal data;
- maintains confidentiality; and
- has mechanisms to:
  - notify changes in its privacy policies;
  - allow the data controller to limit the processing of the personal data;
  - have security measures that are reasonable with respect to the service;
  - guarantee the cancellation of data once the service is terminated; and
  - block access to the personal data by persons that do not have access privileges except when ordered by a competent authority and the data controller is informed of such order.

Finally, another essential obligation is that data controllers must appoint a data protection officer or department to answer data subjects’ access, rectification, suppression and rejection requests.

VIII YEAR IN REVIEW

The first authorisation in Mexico to a fintech entity to operate as an e-money company was granted by the CNBV in January 2020. Fintechs that were carrying out electronic payment funds or crowdfunding activities had to file their authorisation request under the grandfathering provision of the Fintech Law no later than September 2019 in order to continue to perform their activities in Mexico during review of their application. Approximately 85 entities filed for their authorisation request in September 2019, and authorisations will continue to be granted in the coming months.
As the number of participants increases, the fintech market will evolve. The application and interpretation of the Fintech Law by the competent authorities remains unknown as they are too becoming acquainted with the industry. However, we expect authorities to be flexible and to promote fintech activities.

Fintech remains an area of interest to the government given that it has proven to be more flexible than banking institutions, allowing the unbanked population to have access to financial services.

IX OUTLOOK AND CONCLUSIONS

As the Fintech Law is a principle-based law, most issues are resolved and understood with secondary regulation and regulatory interpretation.

It is likely to be an environment of constant change supported by cooperation and new developments within the fintech market; we predict that new actors will enter the market and will be interested in the way fintech services will be conducted. We expect that more banks will, in a cautious manner, begin providing fintech services, as many people have shown interest in the market.

Regarding the adoption of tokens and cryptocurrencies within Mexico, the general expectation was that Banxico would allow e-money companies’ customers to transact with cryptocurrencies. Banxico’s rationale for prohibiting fintech entities and credit institutions from providing cryptocurrency transfers and custodial services is prompted by its concern that fintech entities could misinform customers or that customers would not be able to understand the mathematical information behind cryptocurrencies and the manner in which their value is determined. It is also seeking to reduce money laundering and terrorism financing risks.

It is not clear whether methods that are provided in the Fintech Law relate to innovative models; we consider that the market will dictate the application of the law and other provisions issued by the financial authorities.

We expect that 2020 will be a year of change and progress in this field and, given the rapid adoption of fintech and the interest the public has shown in it, we foresee that Mexican users and service providers are likely to continue to increase rapidly.
Chapter 16

NETHERLANDS

Martijn Schoonewille, Wendy Pronk, Marije Louise, Mariska Kool and Pepijn Pinkse

I OVERVIEW

The Netherlands has a strong presence in the fintech ecosystem. At present, a large number of companies and service providers are active in this sector. In fact, factors like a strong and stable financial sector, striking adoption rate in innovative technology and rapidly growing tech start-ups make the Netherlands an ideal hub for fintech companies.

This appeal is further enhanced by the Dutch tax regime. It includes a broad exemption for dividend income and absence of withholding taxes on interest and royalty payments. For companies realising a limited taxable profit (up to €200,000), a reduced corporate tax rate applies of 20 per cent, which will be gradually lowered to 15 per cent in 2021 (the headline rate is 25 per cent, reduced to 20.5 per cent in 2021). The Netherlands further stimulates innovation with a innovation box regime, which in essence applies a tax rate of 7 per cent to certain profits realised by R&D activities. Wage tax benefits can apply to reduce R&D labour costs, which benefits the employer. Employees relocating to the Netherlands may also benefit from a reduction in their effective income tax burden, subject to certain conditions.

The regulatory approach to fintech in the Netherlands can be described as encouraging and fintech-friendly. As in a number of the adjacent jurisdictions, the Netherlands has a twin peaks supervision model. This model focuses on conduct of business supervision on the one hand and system supervision and prudential supervision on the other hand. Whereas the Dutch Central Bank (DCB) is the competent regulator for system and prudential matters, the Netherlands Authority for the Financial Markets (AFM) is the competent regulator responsible for the conduct of business supervision.

Both supervisors are well aware of the chances, but also the risks that come along with new technological developments. They assist market players in applying the existing regulatory framework to new services and products and flag gaps that may require further amendment of such a framework by the Dutch legislator. This leads to an environment in which fintech players and solutions can thrive, albeit that the supervisors sometimes struggle with the (lack of) ability to apply the applicable rules proportionally.

Martijn Schoonewille is a partner and Wendy Pronk, Marije Louise, Mariska Kool and Pepijn Pinkse are senior associates at Loyens & Loeff NV. The authors also wish to thank Joanne Zaaijer and Iram Velji for their invaluable contribution in respect of the data protection laws and regulations in the Netherlands. The information in this chapter is accurate as of April 2019.
II REGULATION

i Licensing of fintech companies

In the absence of a specific fintech licence in the Netherlands, it should be assessed whether fintech companies fall within the existing legal framework which aims to regulate the provision of traditional financial services. The Netherlands does not have one act that includes all rules relating to fintech businesses. However, the Dutch Act on Financial Supervision (AFS) and its further regulations are considered the main statute when it comes to financial regulatory laws in the Netherlands. Many of the rules contained in the AFS implement the European directives, such as Payment Services Directive (PSD) II, Electronic Money Services Directive II, Markets in Financial Instruments Directive (MiFID) II, Undertakings for Collective Investments in Transferable Securities (UCITS) V and Alternative Investment Fund Managers Directive (AIFMD). Whether a fintech company falls within scope of such framework depends on the exact activities. One example is a crypto-exchange on which trading can take place in Bitcoin futures. Such futures qualify as financial instruments, as a result of which the exchange in principle requires a licence as an investment firm for operating a trading venue. If only cryptocurrencies can be traded on the crypto-exchange that do not qualify as financial instruments, the exchange falls (currently) in principle outside the scope of regulation.

Further developments are expected in the regulation of fintech companies. In a recent joint report, DCB and the AFM recommended the introduction of a licensing regime for fiat-crypto exchange platforms and wallet providers to ensure effective implementation of the Fifth Anti-Money Laundering Directive (Directive (EU) 2018/843, AMLD V), amend the European regulatory framework to enable blockchain-based developments of SME funding and introduce a European definition of a security.

ii Marketing of fintech products and services

There are no specific marketing rules for fintech products and services. Whether or not fintech companies are subject to marketing rules depends on the qualification of the products and services they offer as regulated financial products and services. In general, financial undertakings have to ensure that any information regarding their products and services is clear, correct and not misleading. Furthermore, sector-specific rules may apply to pre-contractual information and marketing material. For marketing materials of certain investment funds, it is, for example, mandatory to include a risk warning, and the way in which forward-looking statements may be presented to clients is prescribed.

iii (Semi-)automated digital advice

The provision of (semi-)automated digital advice or ‘robo-advice’ may be subject to a licence obligation as (1) a financial adviser on the basis of Section 2:75 AFS where it concerns advice to consumers (or clients where it concerns insurance products) on financial products, or (2) an investment firm under the Dutch implementation of MiFID II (Directive 2014/65/EU), if advice is provided to clients on financial instruments. The AFM has published guidance on the provision of robo-advice on financial products. According to the AFM, robo-advice can improve the accessibility and quality of advice on products in non-complex customer

---

situations. In respect of more complex situations or when integral advice is required on the financial situation of a customer, the AFM still sees added value in physical advice. The AFM also published guidance on the duty of care in case of (semi-)automated asset management.

iv Credit information services

Fintech companies that provide credit information services, such as offerors of credit comparison websites, may be subject to a licence obligation as a credit intermediary on the basis of Section 2:80 AFS. The performance of intermediary services is broadly defined and covers both activities aimed at the conclusion of a credit agreement between a credit offeror and a consumer and assistance in the servicing of such credit agreement. In its guidance on when companies are considered to be intermediaries, the AFM makes the distinction between intermediaries and lead generators. The latter solely receives and passes on the consumer’s name, address, telephone number and email address to the credit offeror, and is as such not involved in the conclusion of the credit agreement. If a fintech company provides more information to the credit offeror than the name and address details, for instance information on the desired credit amount, the licence plate of the car which the consumer will buy or details on the financial situation of the consumer, the fintech company will likely be regarded as a credit intermediary.

v Cross-border issues

In general, Dutch licence requirements apply to fintech companies that offer regulated products and services ‘in or from the Netherlands’. As a result of this geographical scope, companies with their registered seat in another EU Member State or a third country that provide services (to clients) in the Netherlands may come in scope of the Dutch regulatory framework.

A licensed company with its registered seat in another EU Member State can be active in the Netherlands without triggering additional licence requirements in the Netherlands if it can make use of a European passport. Generally, to make use of the European passport, the licensed company has to inform its home state regulator on its intention to provide cross-border services to the Netherlands or to open a branch office in the Netherlands. Examples of services for which a European passport is available are investment services, banking services, payment services, insurance intermediation and fund management services. However, if, for example, a credit agreement is concluded with a Dutch consumer by a credit offeror that is not a bank and with its registered seat outside the Netherlands, this in principle requires a local licence in the Netherlands.

Third-country fintech companies seeking to be active in the Netherlands are generally subject to licensing requirements, unless a specific exemption applies. Whether or not it is relevant that services or products are actively marketed to Dutch clients depends on the type of service or product provided. Under the AIFMD (Directive 2011/61/EU) and MiFID II, a licence requirement is triggered if Dutch clients are actively targeted by the third-country fintech company. If Dutch clients (under MiFID II) or professional investors (under the AIFMD) are accepted on the basis of reverse solicitation, this will generally not trigger Dutch licence requirements.

5 AFM, ‘Publicatie bemiddelen.’, September 2014.
III DIGITAL IDENTITY AND ONBOARDING

i Digital identity

While numerous private enterprises are introducing various forms of digital identity, the only generally recognised method is currently ‘DigiD’ (Digital Identity), which is issued by the Dutch State. DigiD is accessible to all residents in the Netherlands, and enables them to make use of the electronic services of several government institutions and organisations that perform public services in the Netherlands (e.g., filing tax return). DigiD cannot be used for transactions.

The Dutch government is currently working on new legislation: the e-Government Act,6 which aims to ensure a more safe and reliable method for Dutch citizens and companies when logging into (semi)government online platforms. To realise this objective, the Dutch government has introduced an electronic identification medium known as eID (electronic identification), which will also meet the strict security measures as stipulated under the European eIDAS Regulation.7 The e-Government Act will become mandatory for the Dutch government, as well as for various industries regulated by the government (e.g., healthcare providers). The new legislation is currently under review by the Dutch House of Representatives, and is expected to enter into force mid-2019.

In addition, in 2016, Dutch banks developed an identification and login service together with the Dutch Payment Association (iDIN). With the use of iDIN, retail account holders can identify themselves online and login at participating organisations (iDIN-acceptants). iDIN meets the requirements under the eIDAS Regulation and the General Data Protection Regulation (GDPR).

ii Onboarding

The AFM and DCB qualify the situation in which the client is not physically present for verification of its identity, without extra guarantees, such as qualified electronical signatures, as high-risk. The AFM acknowledges that identification can take place from a distance by means of innovative technologies.8 It refers in that respect to the opinion of the European Supervisory Authorities (ESAs) in relation to the use of innovative solutions by financial undertakings in the customer due diligence process.9

In this opinion, the ESAs discuss that innovative solutions often involve non-face-to-face verification of customers’ identity on the basis of traditional identity documents through various portable devices such as smartphones or the verification of customers’ identity through other means, for example, central identity documentation repositories (often referred to as ‘KYC utilities’). The ESAs encourage competent authorities to support those developments while also discussing the risks attached to these innovative solutions. In order to mitigate these risks, they note for example the possibilities to add a physical element in digitised

---

8 AFM, Leidraad Wwft, Wwft BES en Sanctiewet, 25 July 2018, as amended per 2 January 2019, pp.20–21. At the time of writing, DCB has not published its updated guidelines in respect of customer due diligence yet. These are expected in Q1 2019.
onboarding of clients, such as a live chat solution, biometrical facial recognition by means of a webcam or the use of software that can detect images that are or have been tampered with (e.g., facial morphing). If the services are offered without any physical interaction, financial undertakings should be aware of the higher risks that are attached to this way of distribution (e.g., identity fraud, the risk that the customer is intimidated, threatened or under duress or geographical risks). Financial undertakings could, for example, make use of a qualified electronical signature in line with the eIDAS Regulation, confirm the identity of a client by sending a letter to the customer’s verified home address, make use of voice-analysing software or combine different identification means.10

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i Collective investment schemes

Collective investment schemes may be subject to the Dutch implementation of the AIFMD or UCITS V (Directive 2009/65/EU, as amended by Directive 2014/91/EU). Under the Dutch implementation of the AIFMD, it is required to obtain a licence when:

- managing a Dutch alternative investment fund (AIF);
- marketing units in an AIF in the Netherlands; or
- for Dutch managers, when managing AIFs or marketing units in AIFs.

For Dutch managers, it is possible to register pursuant to the ‘small managers registration regime’ as a result of which no licence has to be obtained. Dutch managers can register pursuant to this regime provided that the assets under management do not exceed certain thresholds and certain marketing restrictions are taken into account (e.g., the units are only marketed to professional investors within the meaning of Section 1:1 AFS).

ii Crowdfunding

Crowdfunding and crowd-lending (also referred to as investment-based and loan-based crowdfunding) are both seen as important new funding means in the Netherlands. With loan-based crowdfunding, the project owner enters into a loan agreement with the crowdfunder or the crowdfunding platform. In the case of investment-based crowdfunding, the project owner issues either equity or debt instruments to the crowdfunder or crowdfunding platform.

There is no specific crowdfunding framework in the Netherlands. Instead, existing regimes, for example, for the provision of investment services or the offering of consumer credit, have been tailored to the use of such regimes for crowdfunding platforms. Certain licensing or registration obligations may be triggered. For example, crowdfunding platforms that are used for the provision of loans to consumers must obtain a licence for the offering of credit pursuant to Section 2:60 AFS, or alternatively, a banking licence pursuant to Section 2:11 AFS if the crowdfunding platform itself attracts repayable funds from the public. Crowdfunding platforms that only provide intermediary services in respect of attracting repayable funds from the public may obtain a dispensation from the AFM to conduct such

activities.11 If a crowdfunding platform receives and transmits orders in financial instruments issued by the project owner, it will require obtaining a licence as an investment firm from the AFM. The applicable regime therefore depends on the type of activities that the crowdfunding platform conducts and the structure that is being applied. The possibilities for crowdfunders or crowd-lenders to freely trade their loans or securities on the secondary market may be restricted in the Netherlands.12

### iii Payment services

The provision of payment services is regulated by the Dutch implementation of PSD II (Directive (EU) 2015/2366). Providers of payment services in the Netherlands require a licence from the Dutch Central Bank pursuant to Section 2:3a AFS, unless they operate on the basis of a EU passport. In addition, banks and electronic money institutions may provide payment services in the Netherlands on the basis of their licence without obtaining an additional licence. PSD II was implemented in the Netherlands on 19 February 2019.13

As part of the Dutch implementation of PSD II, banks have to cooperate when a user of an online bank account wants to provide third-party providers with access to such bank accounts.14

### V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

#### i Regulation of cryptocurrencies

Since cryptocurrencies do not qualify as a legal currency or electronic money and in the absence of a specific legal framework for cryptocurrencies at the level of the EU and the Netherlands, the current viewpoint is that cryptocurrencies (i.e., cryptoassets without an issuer) do not fall within the scope of Dutch financial regulation. This may be different for instruments or contracts that have cryptocurrencies as their underlying value, such as the Bitcoin future that qualifies as a financial instrument.

#### ii Regulation of tokens

Dependent on the characteristics, tokens may qualify as securities or another type of financial instrument, such as a unit in an investment fund or a derivative instrument. A case-by-case assessment needs to be made taking into account the specifics of the token at hand.

A utility token, which is structured as a prepaid right to receive a service or good from the issuer of the token, typically falls outside the scope of supervision. On the other hand, a security token may qualify as a security, for instance in case of a profit-sharing right.15

A security is defined in Section 1:1 of the AFS, inter alia, as a transferable share, or other

---

11 M Williams, Peer-to-peer lending in the Netherlands, Journal of European Consumer and Market Law, p. 188.
14 Accidentally, this obligation did not enter into force on 19 February 2019. This has been repaired by the amendment of the decree mentioned in footnote 13.
similar transferable instrument, or a transferable bond or other transferable debt instrument. Recently, the supervisors have suggested bringing the Dutch law definition of ‘security’ more in line with the definition of security at the European level, which would make it broader.

iii Money-laundering rules for cryptocurrencies and tokens
Under the current anti-money laundering legislation, certain financial institutions are subject to client due diligence controls. Fintech companies that do not provide regulated services or products do not typically fall within the scope of such legislation. Under the implementation of AMLD V, it is expected that virtual currency platforms will be included in the definition of ‘obliged entities’. Consequently, virtual currency exchange platforms will have to apply customer due diligence controls each time virtual and fiat currencies are exchanged, which effectively puts an end to the anonymity of virtual currency users. Also, custodian wallet providers will be qualified as obliged entities. AMLD V was to be implemented in Dutch legislation in January 2020.

iv Marketing of cryptocurrencies and tokens
Depending on the qualification of cryptocurrencies and tokens, specific marketing rules may apply. The offering of securities to the public in the Netherlands is for example prohibited, unless an approved prospectus is made generally available or unless an exemption applies. General consumer and investor protection regulations may apply independent of the qualification of the token or cryptocurrency as a regulated financial product. These regulations provide that the offeror of the tokens or cryptocurrencies should properly inform investors in the token offering or initial coin offering (ICO) to enable them to make an adequate assessment of the investment, for instance by issuing a white paper that does not only highlight the advantages of the offering but also potential risks and downsides.

v Tax treatment of cryptocurrencies and tokens
In the Netherlands, as in most jurisdictions, there are no specific tax laws on the taxation of cryptocurrencies. The tax treatment is based on general principles and guidance issued by the Dutch Tax Authorities.

For Dutch tax purposes, cryptocurrencies are not formally treated as money or liquid assets, but as (current) assets. As a corporate entity is deemed to carry out its business with all its assets, cryptocurrencies are deemed part of the business enterprise of the corporate entity (irrespective of the business it operates). This means that realised gains are taxed and losses are tax deductible. Cryptocurrencies on the balance sheet are valued at cost price or lower market value. If a corporate entity receives payments in cryptocurrency, these have to be converted to euros (or another functional currency if applicable).

No specific rules exist for the Dutch tax treatment of tokens. This means that the existing tax law framework has to be applied to tokens. In general, it can be expected that payments for utility tokens will be deemed as advance payments that do not have to be reported as taxable profit yet. Security tokens are generally qualified as equity or debt, depending on the characteristics of the token.

It can generally be stated that, if a token contains a repayment obligation, it could be considered as debt for corporate law purposes. However, Dutch tax law may still qualify such

16 Letter of the State Secretary of Finance published on 28 May 2018.
debt instruments as equity for Dutch tax purposes. Dutch Supreme Court case law\(^{17}\) dictates three specific situations in which a repayment obligation formally exists, but is ignored for tax purposes. Most notably, this is the situation if a debt instrument has a profit-dependent interest rate, has a term of over 50 years and is junior to other debt. The other two situations are the sham loan (equity is actually intended) and the bottomless pit loan (it is immediately apparent that no repayment will ever take place). In such situations, Dutch tax law requalifies such corporate law debt instruments to equity. One of the key differences between debt and equity for Dutch tax purposes is that interest payments are generally tax deductible for the payor and taxable at the hands of the payee. Conversely, dividend payments are not tax deductible for the payor, nor is dividend income usually taxed (depending on certain conditions). Another key difference is that dividend payments are in principle subject to Dutch dividend withholding tax, although in various cases exemptions may apply.

VI OTHER NEW BUSINESS MODELS

i Self-executing contracts

Under Dutch law, it is possible to conclude self-executing contracts or ‘smart contracts’. There is no specific legal framework applicable to smart contracts. A smart contract can be seen as a computerised algorithm that automatically performs the terms of the contract. Smart contracts typically have the characteristics that execution is automated and performance is ensured without recourse to legal remedies. An example in the financial sector is a smart contract for a flood insurance policy, whereby insurance claims are paid out automatically if the policy is triggered on the basis of a linked data set. Smart contracts are not suitable for all types of agreements, since it may be difficult to convert the contractual agreements into computer code that follows the logic of ‘if A then B’.

ii Third-party comparison websites

Third-party comparison websites that compare regulated financial products or services may be subject to a licence obligation as an intermediary (see Section II.iv). If personal data of interested customers is processed, then the third-party comparison website has to comply with the GDPR\(^{18}\) and the Dutch GDPR Implementation Act.\(^{19}\) In general, third-party comparison websites must check the information of offerors of regulated products to ensure that it is complete and reliable. The Netherlands Authority for Consumers & Markets takes the view that price transparency rules also apply to third-party comparison websites.\(^{20}\)

---

20 ACM, ‘Vergelijkingssites financiële producten.’, February 2012.
VII INTELLECTUAL PROPERTY AND DATA PROTECTION

i Data protection

In the Netherlands, client data is protected under various data protection rules. This includes the GDPR and the Dutch GDPR Implementation Act, the Protection of Business Secrets Act (PBSA)\(^{21}\) and the Law to Protect Networks and Information Systems (LPNIS),\(^{22}\) as further described below.

Client data that relates to an identified or identifiable natural person (e.g., bank account details but also owners and representatives of a company) qualifies as personal data\(^ {23}\) and is protected under these laws. Data relating to legal entities and deceased\(^ {24}\) individuals do not fall within the scope of the GDPR or the GDPR Implementation Act.

Companies falling under the scope of the GDPR and the GDPR Implementation Act are accountable for processing personal data with a lawful basis\(^ {25}\) and with transparency, integrity and confidentiality. For instance, customer due diligence activities must be based on a statutory data processing ground and must be proportionate to its aim. In addition, data subjects (meaning the individuals to whom the personal data relates to) must be informed on the data processing activities carried out. There are no special rules that apply to digital profiling of clients under the GDPR. However, the GDPR does apply to automated processing of personal data that evaluates certain things about an individual (profiling) and sets out certain rules for such processing activities. For instance, such processing may require an individual’s explicit consent.

The PBSA provides companies with a tool to protect their confidential know how and other business information. This can include any type of information, including client data. However, the information must be secret, must have a commercial value and must be adequately protected in order to qualify as a business secret, thereby falling under the scope of this Act.

The LPNIS requires providers of essential services and of digital services to implement measures that decrease the likelihood of cyber-incidents occurring. These measures should also ensure minimum negative consequences in the event that such incidents occur. This law also requires companies to report serious incidents to the Ministry of Justice and Safety, which is the incidents response team in the Netherlands.

ii Intellectual property rights

Several types of intellectual property rights may play a role when it comes to protecting fintech business models and related software. The most relevant type is copyright protection. In extraordinary cases, patent protection may be available as well. When a business model is not eligible for copyright protection or copyright protection, the PBSA may still provide protection of such a business model.


\(^{23}\) Article 4, GDPR.

\(^{24}\) Recital 27, GDPR.

\(^{25}\) Article 5, Paragraph 1 Sub a, GDPR.
When it comes to copyright protection, the Dutch Copyright Act (DCA)\(^{26}\) requires that a work has an ‘original character’ and ‘bears the personal mark of the author’. This is, in essence, the same criterion as the criterion developed by the European Court of Justice in the Infopaq judgment (16 July 2009): a work must be one’s ‘own intellectual creation’. A basic principle under the DCA is that mere ‘ideas’ do not qualify for copyright protection as such. Ideas need to be worked out in detail to become copyright protected. If a certain work has sufficient originality, it is automatically protected by the DCA. There are no registration formalities in the Netherlands.

With respect to software, the DCA explicitly provides that software and material to prepare software is eligible for copyright protection. The copyright protection of software programs applies to the expression (in any form) of a computer program. Equal to the aforementioned basic principle, ideas and principles that underlie elements of a computer program, or ideas that underlie interfaces, are not copyright protected. This means that financial company A and financial company B can have, in essence, the same software solution in place, while both solutions have been programmed in a different manner (have a different source code), by different persons (but with the same underlying ideas).

While it is relatively easy to qualify for copyright protection, qualifying for patent protection is a different – and complex – story. Software as such (the program ‘stand-alone’ or ‘as such’) cannot be protected by a patent in the Netherlands (nor in the European Union). If the software has a certain ‘technical effect’ – when it is for instance implemented in hardware and directs or determines a certain movement of such hardware – it may be eligible for patent protection included in the technical solution as a whole. The threshold for obtaining patent protection is, however, still rather high and process of obtaining patent protection is time consuming. During the application process, it will be assessed whether the technical solution is sufficiently ‘new’ as compared to existing solutions to the same problem. The technical solution may not be incorporated in prior art.

The copyrights to a certain software program are automatically attributed to the employer if an employee develops the software in the course of his or her employment. The same more or less applies to patentable inventions made by an employee in the course of his or her employment. In case of the latter, the Dutch Patent Act explicitly provides that the employee should be paid a reasonable compensation for the invention based on the financial interest of the invention. With respect to copyrights, the DCA does not require a reasonable compensation for the employee.

Financial companies that hire independent contractors for developing fintech business models or software, should arrange for the transfer of the copyrights that come into existence during or after the development by written contract. Otherwise, the independent contractor will be the owner of the copyrights. Patent protection will only be obtained after application and subsequent registration, but it is advisable to agree with an independent contractor in writing that only the client (in this case the financial company) shall be allowed to apply for patent protection.

---

VIII YEAR IN REVIEW

The year 2018 and the beginning of 2019 can be characterised by a further development of the regulation and legal treatment of fintech in the Netherlands. Both the AFM and DCB are following new developments closely and are providing guidance to market players, for example, through the InnovationHub. In the course of 2018, the AFM published its vision and guidance in respect of robo-advice and (semi)automatic portfolio management, while DCB is heavily involved in the practical implementation of PSD II. With the entry into force of PSD II on 19 February 2019, new fintech players may be welcomed in the Dutch arena of payment services.

In addition, a consultation proposal was published in December 2018 for the implementation of the Fifth Anti-Money Laundering Directive. This proposal introduces a registration requirement for virtual currency exchange platforms and custody wallet providers in the Netherlands. In addition, the AFM and DCB published their recommendations for a regulatory framework for cryptos in January 2019.

At European level, some developments are taking a bit longer than expected, such as the development of the new European regime for crowdfunding services providers, but others are moving in a faster pace, such as the development of the thoughts on a new framework for cryptoassets.

From a more commercial perspective, the attitude of ‘wait and see’ of the Dutch legislator and supervisors and the ability to have open conversations with them, together with macro-economic developments like Brexit, have made the Netherlands an appealing jurisdiction for new market players to set up their operations. Accordingly, we have seen a large increase in the number of regulated companies that are active in the Netherlands.

IX OUTLOOK AND CONCLUSIONS

Based on the fast pace in which the regulatory framework and the AFM and DCB are adapting to fintech solutions and players, it may be expected that the future will be characterised by further integration of fintech in the Dutch financial markets. Not only do we expect a further development and maturation in the products and services that are offered by incumbents and start-ups, but also in the outsourcing of certain back-office functions (such as compliance, AML/KYC and transaction reporting) to specialised IT providers. For 2019 and 2020, we expect further growth in payment solutions and more clarity on the regulation of security tokens.

27 See the register that has been set up by the European Banking Authority (EBA), which is accessible through its website (https://euclid.eba.europa.eu/register/search).
Chapter 17

PORTUGAL

Tiago Correia Moreira, Helena Correia Mendonça, Conceição Gamito, José Miguel Carracho and Francisca César Machado

I OVERVIEW

The regulatory treatment of fintech-related matters in Portugal greatly depends on the legal qualification of the different types of fintech companies or the products and services being offered.

The main legal and regulatory fintech concerns are those directed at payment services and e-money related activities, as well as at crowdfunding platforms. The two current major categories of fintech companies are payment services institutions and e-money issuers, both regulated under Decree-Law No. 91/2018, of 12 November, enacting the Payment Services and E-Money Legal Framework (PSEMLF), which transposed Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 (the PSD2) to the Portuguese legal framework. The PSEMLF, in light of the PSD2 transposition, also created the necessary regulation for third-party providers such as Payment Initiation Service Providers (PISP) and Account Information Service Providers (AISP) to enter the Portuguese market. Crowdfunding platforms, in turn, are regulated by Law No. 102/2015 of 24 August and Law No. 3/2018 of 9 February, as well as by Portuguese Securities Market Commission (CMVM) Regulation 1/2016 and Ministerial Order No. 344/2015 of 12 October.

The Portuguese legislator and regulatory authorities’ approach to fintech has been somewhat neutral, which resulted in the late transposition of Payment Services Directive 2 (PSD2) (a delay of almost a year from the deadline of 13 January 2018). There is also no legal approach for testing financial technology under a sandbox regime as of now. This is also true from a tax perspective, where no specific Portuguese legal regime exists on tax incentives for fintech-related matters.

Notwithstanding this, the Portuguese financial regulators (i.e., the Bank of Portugal, the CMVM and the Insurance and Pension Funds Authority) have recently implemented the Portugal FinLab programme, which is now in its second edition, with the purpose of establishing an easily accessible communication channel between entrepreneurs and emerging companies and the financial regulators, aimed at supporting the development of fintech businesses and companies in navigating the legal and regulatory challenges and concerns posed by the regulators. Additionally, there has also been increased interest in these matters by the regulators, which have participated in fintech-related conferences and disclosed information released during these conferences on their websites.

1 Tiago Correia Moreira is a partner, Helena Correia Mendonça is a principal consultant, Conceição Gamito is a senior adviser and José Miguel Carracho and Francisca César Machado are associates at Vieira de Almeida (VdA). The authors would like to thank André Marques Piteira (an associate in the IP department), David Paula and Sebastião Barros Vale (associates in the ICT department).
II REGULATION

i Licensing and marketing

The PSEMLF sets out the applicable rules and requirements for the incorporation and licensing of payment institutions and e-money issuers as well as PISPs and AISPs, all being subject to the Bank of Portugal’s supervision. For that effect, certain mandatory legal documentation must be filed with the Bank of Portugal, including, inter alia, draft by-laws, business plan, share capital commitment, corporate structure and beneficial ownership, the managers’ identification and fit and proper documentation, as well as corporate governance and internal compliance models and procedures. Current minimum statutory share capital requirements applicable to payment institutions ranges from a minimum of €20,000 to €125,000 (depending on the type of services provided) and a minimum of €350,000 for e-money institutions. PISPs are required a minimum statutory share capital €50,000 and AISPs are required to hire an insurance policy or other similar guarantee scheme covering their activity in Portuguese territory in the case of breach or unauthorised access to data.

All marketing and advertising carried out by these entities must abide by the general rules applicable to marketing and advertising by banks and other financial institutions. This means that, among other requirements, all marketing and advertisement products and materials must clearly identify the offering or advertising entity while ensuring that the main features and conditions of the marketed products or services are easily perceived by targeted consumers.

The PSEMLF provides for an extensive list of products and services that may only be offered or rendered by either payment or e-money institutions, as well as PISPs or AISPs. This means that, in practice, considering the nature and business model of most fintech companies and the services they offer, such entities will have to qualify under Portuguese law as one of these entities (being that an entity securing an e-money licence ensures that it can render all services regulated under the PSEMLF, provided it requires an authorisation to that effect when registering with the Bank of Portugal), having thus to comply with its regulatory framework.

In what concerns crowdfunding platforms, Portuguese law sets out the requirements and conditions for the corporate entities managing crowdfunding platforms, which are subject to the CMVM’s supervision when they are either collaborative equity-based or loan-based platforms. These entities are subject to prior registry and authorisation with the CMVM. The submission shall be accompanied by the relevant required documentation, which includes, inter alia, the corporate details, structure and beneficial ownership, managers’ identification and fit and proper documentation, business plan and model, indication about whether it should be considered a financial intermediary or an agent thereof, as well as evidence of compliance with the minimum financial requirements. Upon registration these minimum financial requirements must be either (1) a minimum share capital of €50,000; (2) an insurance policy covering a minimum of €1 million per claim, and a minimum of €1.5 million in aggregate claims per year; or (3) a combination of both (1) and (2) that ensures proper similar coverage.

ii Cross-border issues

Payment or e-money institutions based abroad may render their services in Portugal, subject to prior authorisation and registry with the Bank of Portugal. The applicable requirements and procedures may vary according to the origin state, as entities based in EU Member States...
may choose to render their services in Portugal either through a branch registered in Portugal, through authorised agents based in Portugal (notably in what concerns e-money distribution) or under a licence granting them the freedom to provide services.

Should the applying entity be based in a third-country state, it shall incorporate a branch or, alternatively, incorporate a legal entity subsidiary in Portuguese territory (following the relevant, though more demanding, procedure).

In relation to crowdfunding platforms, no cross-border regime has yet been enacted under either European or Portuguese law; this lack of passporting regime requires foreign crowdfunding platforms interested in acting in the Portuguese market to complete the Portuguese registration process with the CMVM (adjusting, for such purpose, the relevant internal documents to meet the Portuguese law requirements) in order to obtain the required local registration. This has been the process applied by the CMVM to cross-border crowdfunding platforms acting in Portugal that are registered with the CMVM and with the competent authority of its home Member State. The latest news in this respect indicates that the CMVM will likely wait for the next developments in the proposed European regulation on crowdfunding service providers, which, among other matters, envisages a more harmonised and standard approach to cross-border activities by these entities.

III DIGITAL IDENTITY AND ONBOARDING

Portuguese citizens must have a citizenship card containing data relevant for their identification (such as full name, parentage, nationality, date of birth, gender, height, facial image and signature). This card also includes the civil identification number, the taxpayer number, the user number for health services and the social security number (Law No. 7/2007, which creates the citizenship card, as amended). The citizenship card proves the identity of its holder before any public and private authorities and entities, through two mechanisms:

a by means of reading the visible elements of the card, together with the optical reading of a specific area of the card destined to such reading (its reading is, however, reserved, mainly, to entities or services of the state or public administration); and

b by means of electronic authentication.

The citizenship card further allows its holder to unambiguously authenticate the authorship of electronic documents by means of an electronic signature. The card contains a chip where additional information is available, such as address and fingerprints – it is in this chip that the certificates for secure authentication and for the qualified electronic signature are available. Hence, the holder of a Portuguese citizenship card has two digital certificates: one for authentication and another for e-signature. However, while the authentication certificate is always activated when the card is delivered to its holder, the e-signature certificate is of optional activation, and such activation can only be done by citizens who are at least 16 years old. A citizen who wishes to use the certificates shall insert his or her PIN in the device requesting or permitting the use of such authentication (or signature) method.

Law No. 7/2007 expressly refers to Regulation 910/2014 on electronic identification and trust services for electronic transactions (the eIDAS Regulation), indicating that the provisions therein established apply to the certificates. Portuguese law on the citizenship card thus already acknowledges the eIDAS Regulation. However, when it comes to trust services, especially e-signature, Decree-Law No. 290-D/99, as amended, continues to be the legislation containing the details on e-signature.
It is important to also note that the certificates of the citizenship card are subject to the legal and regulatory rules of the Portuguese State Electronic Certification System (approved by Decree-Law No. 116-A/2006). This system aims to guarantee the electronic security of the state and the strong digital authentication of electronic transactions among the services and bodies of the public administration, as well as between the state and the citizens and companies.

In addition, Law No. 37/2014, as amended, created the ‘digital mobile key’, which is an additional and voluntary means (1) of authentication in portals and sites of the public administration and (2) of qualified electronic signature in the terms indicated in the eIDAS Regulation. All citizens may require the association of their civil identification number to a mobile phone number or an email. Foreign citizens without a civil identification number may also require such association, which is done through their passport number, their tax identification on residence permits (or other documents as indicated in the regime for entry, stay, exit and expulsion of foreigners from the national territory) or their residence card. The digital mobile key is a system for secure authentication comprising a permanent password and a numerical code issued for each use and generated by the system.

Financial service providers, including payment institutions and e-money institutions, may carry out fully digitised onboarding of clients, including, as of recently, by using videoconference procedures.

The Bank of Portugal’s Notice No. 2/2018 allows financial institutions to make use of remote onboarding procedures while complying with the know your customer (KYC) requirements set out under the applicable AML framework. Currently, admissible remote onboarding procedures under applicable AML law and Notice 2/2018 are videoconferencing and other means of KYC and onboarding procedures carried out by qualified trust service providers (the latter being compliant with the framework set forth under Regulation (EU) No. 910/2014).

The Portuguese Data Protection Authority (CNPD) has consistently ruled that companies may only reproduce or take and keep a photocopy of a Portuguese citizenship card with the holders’ consent, expressed in the terms of the General Data Protection Regulation (GDPR) (EU Regulation No. 2016/679 of 27 April). Although Law No. 7/2007 does provide for an exception to this obligation (notably, where the reproduction and storage of the copy of the citizenship card is expressly provided by law), CNPD has clarified that financial institutions that are bound by KYC obligations under AML laws are still required to obtain such a consent, as the law does not expressly refer to the citizenship card as the means of verifying the client’s or the beneficial owner’s identity during an onboarding process. In this regard, financial institutions are advised to offer their clients alternative means of proving their identity, such as by providing a copy of their passports or driver’s licences.

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

Both payment services providers (i.e., payment and e-money institutions as well as PISPs and AISPs) and crowdfunding platforms – either equity or loan based – are subject to licensing and registry requirements with either the Bank of Portugal or the CMVM, respectively.

Although still in a very preliminary phase, owing to the applicable framework having entered into force recently, crowdfunding schemes are gaining some traction, mostly in the loan-based platforms sector, where there are now six crowd-lending platforms registered with the CMVM. Further developments may arise in this field as the market develops and
market players become more sophisticated and numerous, in which case movements towards securitisation of loan portfolios originating from such platforms may eventually begin to be noticed in the medium to long term.

Notwithstanding, current securitisation law (Decree Law No. 453/99, as amended) defines which entities may qualify as originators of receivables for securitisation purposes and these are limited to the Portuguese state and other public legal persons, credit institutions, financial companies, insurance firms, pension funds and pension fund management companies. However, other legal persons that have their accounts legally certified by an auditor registered with the CMVM for the previous three years may also assign loans for securitisation purposes; this may open the door to crowdfunding entities being able to enter into securitisation and other structured finance transactions, which were traditionally reserved to banks and other incumbents. However, owing to the nature of the entities resorting to crowd-lending platforms for funding, as well as those managing such platforms, we envisage that such a movement towards securitisation may still take some time.

In June 2019, Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services came into force. This Regulation places some obligations upon providers of online intermediation services simultaneously (1) constituting information society services, (2) allowing business users to offer goods or services to consumers and (3) provided to business users on the basis of contractual relationships (such as platforms’ terms of use). Obligations include transparency and intelligibility requirements for platforms’ terms and conditions, duties of notification to business users concerning changes to those terms and conditions, limitations on the restriction, suspension and termination of online intermediation services, explanation of ranking parameters (when the online intermediation services include such ranking), transparency about differentiated treatment of business users and about the service provider’s access to personal data through the platform, and setting up an internal complaint-handling system with certain characteristics (without prejudice against the possibility of business users resorting to mediation). The Regulation shall apply across the European Union from the 12 June 2020.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

Blockchain or distributed ledger technology is not subject to specific regulation in Portugal as a technology. Indeed, the focus of regulation brought by blockchain has pertained essentially to a specific sector: banking and finance, including cryptocurrencies and initial coin offerings (ICOs), notably in what concerns investor protection and fraud prevention. There is currently

---

2 In this respect, it is noteworthy that Directive (EU) 2015/1535 of the European Parliament and of the Council, which defines and sets-out rules on information society services, states that this Directive shall not apply to rules relating to matters covered by EU legislation in the field of financial services, as listed non-exhaustively in Annex II to this Directive. This may ultimately raise some doubts about the applicability of Regulation (EU) 2019/1150 to the provision of online intermediation services relating to financial services. The Regulation also states that it ‘shall not apply to online payment services (…) which are not provided with the aim of facilitating the initiation of direct transactions and which do not involve a contractual relationship with consumers’, without prejudice to EU law applicable in the areas of judicial cooperation in civil matters, competition, data protection, trade secrets protection, consumer protection, electronic commerce and financial services.
no regulation concerning the tokenisation of assets in general (and securities in particular, such as bonds or shares), although nothing in the law seems to generally prohibit it. As such, in principle we see no impediment to the tokenisation of assets or credits, provided that parties involved in a given transaction would agree on the dematerialisation of such agreement/title and the underlying assets (and the corresponding representation of such assets by tokens). Notwithstanding this, it would not be applicable in principle to those assets subject to special registration or notarisation formalities (such as real estate assets) as this would additionally entail a formal and legal recognition by the governmental or registration authorities on the correspondence to such dematerialised property titles to the physical/notarial reality which still has no legal framework in place for these cases.

However, the approach in Portugal in this sector has been to generally exclude cryptocurrencies from being qualified as tender or ‘legal currency’ and not issuing specific regulation dealing with them. Both the Bank of Portugal and the CMVM share this understanding and – like the majority of European regulators – are pursuing a wait-and-see approach in anticipation of a possible broader and harmonised European legislation ruling these matters.

Nonetheless, a different case-by-case approach should be taken regarding those assets qualifying as securities, such as security tokens or other hybrid tokens comprising some security-like traits, pursuant to ESMA’s advice from 9 January 2019, whereas cryptoassets qualifying as transferable securities (or another type of financial instrument under MiFID II’s criteria) should be subject to the broader EU financial rules in this respect (including, inter alia, MiFID II, the Prospectus and Market Abuse Directives, etc.). Although the definition of what qualifies as a ‘security’ is mostly committed to national regulation implementing EU legislation, we would envisage the CMVM to follow the same approach as ESMA and deciding on the applicability of the legal framework applicable to securities (including that of public offerings in the case of ICOs) on a case-by-case basis. An example of this approach can be seen in the context of the Bityond ICO in 2018, where the CMVM decided not to apply the public offerings regime (and the securities legal framework as a whole) after having analysed the white paper and the token’s configuration and associated rights and obligations, which did not present similar traits to those of tradeable securities.

However, the Bank of Portugal has, as far back as 2013, issued a clarification under which it considered that Bitcoin cannot be considered secure currency, given that its issuing is carried out by non-regulated and non-supervised entities. In addition, the Bank of Portugal clarified this and stated that the users bear all the risk, as there is no fund or protection scheme guaranteeing depositors’ or investors’ funds. This approach closely follows the position of the European Banking Authority (EBA). Note that specific regulation on cryptocurrencies is not expected soon: both the government and the Bank of Portugal have stated that they will not regulate cryptocurrencies and that the first step shall be taken by the European Commission. In this respect, both ESMA and the EBA sent reports, on 9 January 2019, to

---

4 Following a study by the European Central Bank on ‘Virtual Currency Schemes’, of October 2012. The Bank of Portugal also reiterated, in 2014, that the use of virtual currency brings risks to consumers and, in 2015, advised banks to abstain from buying, detaining or selling virtual currencies (Circular Letter 011/2015/DPG, of 10 March 2015).
5 But, according to the EU Fintech Action Plan published on 8 March 2018, the Commission stated that ‘the case for broad legislative or regulatory action or reform at EU level on fintech issues is ‘limited’.
EU policymakers on ICOs and cryptoassets, assessing and advising the European Commission on the applicability and suitability of EU legislation to said instruments. Notably, EBA's report stresses that:

"Competent [national] authorities have reported to the EBA that it is their understanding that cryptoasset activity levels in their jurisdictions remain low and do not, at this stage, present a threat to financial stability, a finding which aligns with the observations of the Financial Stability Board. However, some issues arise, in particular with regard to consumer protection, market integrity and the level playing field, in view of the fact that: (a) current EU financial services law does not apply to a number of forms of crypto asset activity; (b) specific services relating to cryptoasset custodian wallet provision and crypto asset trading platforms may not constitute regulated activities under EU law; and (c) the emergence of divergent approaches across the EU has been identified. For these reasons, the EBA considers that there would be merit in the European Commission carrying out a cost/benefit analysis to assess whether EU level action is appropriate and feasible at this stage to address the issues set out above."

Additionally, ESMA’s report’s press release states that:

ESMA has identified a number of concerns in the current financial regulatory framework regarding cryptoassets. These gaps and issues fall into two categories:

a For cryptoassets that qualify as financial instruments under MiFID, there are areas that require potential interpretation or re-consideration of specific requirements to allow for an effective application of existing securities and financial regulations; and

b Where these assets do not qualify as financial instruments, the absence of applicable financial rules leaves investors exposed to substantial risks. At a minimum, ESMA believes that Anti Money Laundering (AML) requirements should apply to all cryptoassets and activities involving cryptoassets. There should also be appropriate risk disclosure in place, so that consumers can be made aware of the potential risks prior to committing funds to cryptoassets.

In this light, and considering that gaps and issues identified would best be addressed at the European level, ESMA then suggests that the European Commission either:

a propose a bespoke regime for specific types of cryptoassets (which does not qualify as financial instruments) by means of a Directive, allowing for the tailoring of the rules to the specific risks and issues posed by those cryptoassets; or

b do nothing, which would fail to address the known investor protection and market integrity concerns.

Despite the lack of regulation and supervision, the Bank of Portugal has indicated that the use of cryptocurrencies is not forbidden or an illegal act. Hence, this entity is so far more focused on a preventive and educational approach, by means of alerting to the risks of cryptocurrencies.

Despite this assertion, the Commission is set to assess ‘the extent to which the legal framework for financial services is technology neutral and able to accommodate FinTech innovation, or whether it needs to be adapted to this end’. It further clarified, with relation to crowdfunding, that ‘The EU framework proposed in this Action Plan will offer a comprehensive European passporting regime for those market players who decide to operate as European crowdfunding service providers.'
The CMVM also issued an alert to investors in November 2017 on ICOs, indicating that most ICOs are not regulated – in which case investors are unprotected due to the high volatility and lack of funds, potential of fraud or money laundering, inadequate documentation (most ICOs have no prospectus but only a White Paper) and risk of loss of the invested capital. Still, the CMVM paved the way for regulation according to their specific circumstances.

Considering the above, the usual distinction between the different types of tokens (or rather the rights and obligations that their issuance and possession entail) underlying the transactions may prove useful. Should tokens be used mainly as a means of payment, the approach taken by the Bank of Portugal and EBA is the one to look at. Conversely, where tokens have more similarities to securities, the approach of the CMVM and ESMA is the one to take note of.

Despite a slight lack of regulatory clarity, there seems to have been some progress in acknowledging this situation, given that the recent proposal for amending the AML Directive (Directive 2015/849) extends its scope of application to virtual currencies; namely, to exchange services between virtual currencies and fiat currencies, and to wallet providers offering custodial services of credentials necessary to access virtual currencies. Notwithstanding the proposed amendment to the European AML framework, the Bank of Portugal has clarified that financial institutions are under the obligation to control transfers of funds coming from and going to platforms of negotiation of cryptocurrencies under AML provisions. In this respect, some major banks in Portugal have blocked transfers that have these types of entities as beneficiaries, although some are beginning to allow transfers being made to exchanges that are deemed more trustworthy.

In line with the Court of Justice of the European Union (CJEU)’s interpretation on the VAT treatment of transactions with cryptocurrencies,6 the Portuguese Tax Authority (PTA) recently issued binding rulings7 stating that transactions, such as exchange of cryptocurrency for traditional currency, and vice versa, should be exempt from VAT.8

Binding rulings only bind the PTA towards the taxable person who submitted the ruling request and in relation to the questions specifically raised to the PTA in such request. Following the CJEU’s judgment, which should apply in all Member States, the binding rulings issued by the PTA were an important step forward in the definition of the VAT treatment of Bitcoin transactions. With these binding rulings, entities exchanging cryptocurrencies,

6 CJEU’s case law C-264/14, from 22 October 2015 (Skatteverket v. David Hedqvist). In this case, the CJEU decided that the exchange of Bitcoin for traditional currency qualifies as a supply of services for VAT purposes. As to the question of whether these transactions should be regarded as exempt supplies, the CJEU pointed out that Bitcoin, being a contractual means of payment, cannot be regarded as a current account or a deposit account, a payment or a transfer. Moreover, unlike a debt, cheques and other negotiable instruments referred to in Article 135(1)(d) of the VAT Directive, Bitcoin is a direct means of payment between the operators that accept it. Therefore, the CJEU ruled that transactions, such as exchange of cryptocurrency for traditional currency, and vice versa, should be exempt from VAT under the provision of Article 135(1)(e) of the VAT Directive. The CJEU did not expressly address the subject of whether the exchange of, for example, Bitcoin for a different cryptocurrency should also be regarded for VAT purposes as an exempt supply of services under Article 135(1)(e) of the VAT Directive. However, in our view, the same reasoning applies and the answer should therefore be the same.

7 Binding Rulings 12904 from 15 February 2018 and 14763 from 28 January 2019.

8 Under the provision of Article 9(27)(d) of the Portuguese VAT Code (which corresponds to the transposition of article 135(1)(e) of the European VAT Directive).

© 2020 Law Business Research Ltd
start-ups and users are now in a safer environment in Portugal from a VAT perspective. Buying, selling, sending, receiving, accepting and spending cryptocurrencies in exchange for legal tender currency (and vice versa) will not trigger a VAT liability, which allows economic agents to deal with cryptocurrencies as they would with legal tender currency or other types of money.

Additionally, for personal income tax (PIT) purposes, the PTA had already issued a binding ruling9 stating that any gains derived from the exchange of Bitcoin for legal tender currency (and vice versa) should not be considered income for personal income tax (PIT) purposes to the extent such activity does not constitute a business or professional activity. Indeed, the PTA concluded that gains derived from the sale of Bitcoin would not fall under the concept of capital gains or investment income as defined by the Portuguese PIT Code and, consequently, those gains are not covered by the taxable base of the Portuguese PIT.

VI OTHER NEW BUSINESS MODELS

There has recently been a substantial dynamic in the Portuguese fintech market, with the entering of new players and stakeholders offering new types of services and products. As an example, the past year saw the market entry of fintech companies offering solutions to export and import finance and to exchange currency through innovative services, as well as crowdfunding platforms aimed at specific markets and business – such as the crowdfunding of real estate developments. This movement hints at the growing market that the recently enacted PSEMLF transposing the PSD2 shall further accelerate, opening up new business opportunities for emerging companies in the areas of open banking services, neo-banks and all other innovation-driven solutions occurring in the banking and financial sector today.

However, in the meantime, new fintech companies offering innovative services may struggle with the burdensome procedures imposed by applicable laws and regulations mentioned above (including the licence and registration procedures or AML-related issues).

Despite the above, services resorting to smart contracts do seem to have some legal comfort. Indeed, from 2007 onwards Portugal has had a specific provision dealing with contracts executed by means of computers without human intervention in its E-Commerce Law (Decree-Law No. 7/2004). This provision applies contract law to these types of contracts and further applies to programming errors, malfunctions and distorted messages the legal regime on mistake. Though self-executing or smart contracts are a step further from contracts concluded without human intervention, it seems that they are permitted under Portuguese law – and, what is more, the above provision may be applicable to them. Indeed, there is a general principle in Portuguese law that, unless otherwise provided, contracts are not subject to a specific form. However, no specific legal framework exists on smart contracts.

On the use of artificial intelligence (AI) in the context of novel business models, adding to the rules on automated decision-making highlighted in Section VII below, on 8 April 2019, the European Commission-led High-Level Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence. According to the Guidelines, trustworthy AI should be: (1) lawful – respecting all applicable laws and regulations; (2) ethical – respecting ethical principles and values; and (3) robust – both from a technical perspective and considering

---

9 Binding Ruling 5717/2015 from 27 December 2016.
its social environment. The Guidelines put forward a set of seven key requirements – which are duly developed in the Guidelines – that AI systems should meet in order to be deemed trustworthy. These include:

- **a** human agency and oversight;
- **b** technical robustness and safety;
- **c** privacy and data governance;
- **d** transparency;
- **e** diversity, non-discrimination and fairness;
- **f** societal and environmental wellbeing; and
- **g** accountability.

Additionally, the Portuguese government has also recently approved its National Strategy for Artificial Intelligence – ‘AI Portugal 2030’, which sets out the main general objectives to reach by 2030, including:

- **a** added economic growth: the added value brought by AI technologies to the economic growth should be significant;
- **b** scientific excellence: improve the front-line position in fundamental and applied AI research of Portuguese academia (universities, polytechnics and research institutions) measured in terms of publication impact, international leaderships, and international collaborations; and
- **c** human development: increase dramatically the qualifications of the labour force, in particular technological qualifications, while promoting inclusion and awareness at all levels of education.

The National Strategy does not specifically address, however, the challenges AI will bring to the financial sector. Nonetheless, it is reasonable to assume that the increasing number of public guidelines and recommendations (both at national and international level) will foster investment in and the development of new AI-driven technologies and businesses.

The new European Commission committed to putting forward proposed legislation for a coordinated European approach on the human and ethical implications of AI during its first 100 days in office (i.e., until March 2020). A 19 February Commission White Paper sets out the scope of a future EU regulatory framework and the types of envisaged requirements, notably:

- **a** voluntary labelling;
- **b** training data;
- **c** data and record-keeping;
- **d** information to be provided;
- **e** robustness and accuracy;
- **f** human oversight; and
- **g** specific requirements for certain particular AI applications, such as those used for purposes of remote biometric identification.

In light of the above, there is a considerable degree of uncertainty as to what the binding legal instruments that may be enacted in the coming years and that may impact the use of AI in financial products will look like, both at the European and national level.
VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Protection of fintech can be effected through several means. The protection of software seems to be the most relevant, as fintech technology usually translates into computer systems and applications. Software is protected in Portugal under the same legal rules that apply to copyright protection (according to Decree-Law No. 252/94, which transposed Directive No. 91/250/CEE, later repealed by Directive No. 2009/24/CE, on computer programs, as amended). Copyright on the computer program belongs to the employer if the software is created by an employee in the execution of his or her duties or following the instructions given by the employer. Copyright does not require registry to exist, but this can be done in the General-Inspection for Cultural Activities (IGAC). Software can also be protected by patent in the cases where it meets the criteria to be considered a computer implemented invention, which is an invention whose implementation involves the use of a computer, computer network or other programmable apparatus. In addition, computer-implemented business models can also be patented, to the extent that they are claimed as a technical solution for a technical problem (e.g., automating a response considering the data collected) and involving technical considerations (e.g., the reading of the database). Otherwise, business models are not patentable. All in all, a case-by-case analysis is necessary to determine if protection by patent is feasible.

Technology developed in the context of a fintech business can also be protected as trade secret. Trade secrecy protects against any act of a person that assesses, appropriates or copies (or any other conduct that, under the circumstances, is considered contrary to honest commercial practices), without consent, information that is secret, that has a commercial value due to that fact and that has been subject to reasonable steps, by the person lawfully in control of the information, to keep it secret (for instance, the execution of non-disclosure agreements). Current national legal provisions on trade secrecy are included in the Industrial Property Code – approved by Decree-Law No. 110/2018, of 10 December as reviewed following the transposition of Directive (EU) 2016/943 of 8 June 2016, on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

A computer platform usually also comprises a set of data, as well as visual interfaces. The data may also be protected as a database if the requirements set in law (Decree-Law No. 122/2000, which transposed Directive No. 96/9/CE, as amended, on the protection of databases) are met. Interfaces can further be protected by copyright under the Copyright Code (approved by Decree-Law No. 63/85, as amended) in their look and feel, screen display and individual visual elements, if they all meet the criteria to be protected (mainly, are 'creative'). Copyright protection, in this case, belongs to the employer or the person that orders the creation, if so established or if the name of the creator is not referred to in the work. In this case, the creator may require a special compensation if the creation exceeds the performance of the task or when the creation is used or brings benefits not included or foreseen in the creator's remuneration.

Fintech businesses collect, control and process vast amounts of personal data (including know-your-customer data) and, as a result, they are subject to data privacy rules. These rules are, from 25 May 2018, the ones provided in the GDPR. The GDPR applies not only to Fintech companies established in the EU but also to companies established outside the EU, in case they have customers in the European Union and the processing of the customers' personal data is made in the context of the offering of services to those data subjects, irrespective of whether a payment of the data subject is required. The European
Data Protection Board (EDPB) has clarified, in its Guidelines 3/2018 on the territorial scope of the GDPR, adopted on 16 November 2018, that the intention to target customers in the EU is key to assessing whether entities established outside the territory of the EU are subject to the GDPR.

In some instances, the processing of personal data may require the customer’s consent. Pre-ticked opt-in or opt-out boxes will no longer be allowed, since consent must be expressed through a statement or by a clear affirmative action. The GDPR places onerous accountability obligations on data controllers to evidence compliance, which constitutes a major paradigm shift in the data protection regime. This includes, among others, conduct data protection impact assessments for more risky processing operations (such as those involving the processing of personal data that could be used to commit financial fraud), and implement data protection by design and by default.

These general data protection rules are complemented by banking secrecy and AML rules, which fintech companies will have to observe when providing services to their clients.

Bank secrecy rules determine that disclosure of clients’ personal data protected by banking secrecy (including cross-border transfers) is permitted only with prior customer authorisation or if the disclosure is necessary to obtain one of the following:

a) compliance with a legal obligation that expressly limits those secrecy duties;

b) compliance with judicial authorities’ requests in the context of criminal proceedings; or

c) compliance with a disclosure obligation to the Bank of Portugal, the CMVM or tax authorities, when they are acting pursuant to their respective attributions.

In the past, the CNPD had already ruled in a specific case that all personal data processed by a bank is subject to banking secrecy.

In the case of processing clients’ data for the purposes of anti-money laundering reporting, the disclosure of specific relevant personal data is based upon the fulfilment of a legal obligation, and there is no need to obtain data subject consent. As the concept of ‘client authorisation’ under PSEMLF and the financial institution’s legal framework differs from the concept of ‘consent’ under the GDPR, many banks and other financial institutions opt to collect clients’ authorisation to disclose information covered by banking secrecy in the context of their general client terms and conditions. In the case of processing clients’ data for the purposes of anti-money laundering reporting under Portuguese AML regulations, the disclosure of specific relevant personal data is based upon the fulfilment of a legal obligation, and there is no need to obtain the data subject’s consent.

Another important aspect of data processing in the context of fintech business is the definition of clients’ profiles and business segmentation, as well as automated decision-making based on profiling. Automated decisions that produce effects concerning the data subject or that significantly affect him or her and are based solely on the automated processing of data intended to evaluate certain personal aspects relating to him or her are not permitted.

The GDPR has introduced new provisions to address the risks arising from profiling and automated decision-making. Mainly, under the GDPR, one may only carry out this type of decision-making where the decision is either necessary for the entry into or performance of a contract or authorised by the EU or Member State law applicable to the controller, or, finally, based on the individual’s explicit consent. Where one of these grounds applies, additional safeguards must be introduced, as well as disclosure of specific information about automated individual decision-making to affected data subjects, concerning the logic, significance and envisaged consequences. In a January 2020 response to the MEP Sophie in’
Veld’s letter on unfair algorithms, addressing whether the GDPR was sufficient to protect data subjects from unfair automated decision-making, the EDPB stressed that ‘controllers are obliged to consider all the potential risks that the use or creation of the specific algorithm can potentially pose to the rights and freedoms of natural persons and, if necessary, take measures to address these risks’.

There are also additional restrictions on using special categories of data (such as health-related data or biometric data) for any processing of personal data, which can ultimately impact the way Fintech companies will implement Strong Customer Authentication mechanisms under the PSD2 Regulatory Technical Standards, as the Regulatory Technical Standards suggest the use of the payment service users’ biometric data in that context. The CNPD has consistently ruled that financial data are sensitive data, in the sense that they reveal aspects of an individual’s private life and, thus, said data should be protected under the Portuguese Constitution. As financial data are also considered by the EDPB as data of a highly personal nature, this may ultimately influence the stringency of technical and organisational measures data controllers and processors choose to implement to protect said data, as well as on the need to undergo a data protection impact assessment (DPIA) before commencing processing activities on said data. The processing of financial data may, then, entail the need for a DPIA under the CNPD’s Regulation 1/2018, which lists the processing activities subject to a mandatory DPIA, as the Regulation refers to the processing of data of a highly personal nature in four of its nine cases.

Without prejudice to the above, Portuguese legislation implementing the GDPR has entered into force on 8 August last year. Law No. 58/2019 brings some additional adjustments or restrictions to the rules set out in the GDPR, notably regarding the processing of deceased persons’ personal data, the applicable data storage periods and minors’ consent for data processing. Most notably, and without prejudice to the GDPR’s purpose limitation principle, Law No. 58/2019 allows controllers or processors to keep personal data until the expiration of any statutory limitation periods during which they may need to use the data to demonstrate compliance with legal or contractual obligations.

VIII YEAR IN REVIEW

Fintech-specific regulation has seen major developments during the past 18 months, notably with the much-anticipated and long delayed transposition of the PSD2 into Portuguese legislation. New players in the PISP and AISP business will be expected to appear in the short to medium term, while some incumbent and traditional banks are also beginning to take advantage of the new framework and are starting to provide open banking services to their customers.

Additionally, the new AML law has also seen some developments with the entry into force of Notice 2/2018 of the Bank of Portugal, which sets out further regulation and specific standards regarding AML obligations to be observed by fintech companies (notably concerning reporting obligations, risk-based policies and KYC and onboarding procedures). As previously mentioned, the Bank of Portugal’s notice clarifying the requirements for remote onboarding procedure paves the way for a more dynamic approach to potential fintech customers and the surging of new market players. However, market data shows that this possibility of using a videoconference as a way of complying with KYC obligations is mostly being used by banks owing to the technical and financial demands that such procedure implies.
under the applicable regulation, although newcomers may take advantage of partnerships with third-party qualified trust service providers to go around the costly and demanding infrastructure that videoconferencing encompasses.

The crowdfunding sector keeps growing and evolving, with new platforms being registered and others in the middle of the registration and authorisation procedures, which boosts the fintech market in this area.

Portugal Fintech (a Portuguese association supporting the emerging fintech ecosystem) continues its mission to promote the Portuguese fintech market, gathering fintech, regtech, insurtech and cybersecurity companies in Portugal, fostering their access and visibility with legislators, start-ups, investors, consultants, banks, regulators and other relevant entities. 2019 was also marked by the opening of the FintechHouse by Portugal Fintech, a technological innovation and financial services hub, described as ‘a unique place that aims to be the meeting point of the entire Ecosystem’.

The Portugal FinLab, an acceleration programme providing a communication channel between new players in the market (or even incumbent institutions having innovative tech-based financial projects or products) and the Portuguese regulatory authorities is now in its second edition. Through it, the regulators provide guidelines and support without the usual hurdles to the participants on how to navigate and operate in the regulatory system.

IX  OUTLOOK AND CONCLUSIONS

The recently enacted PSEMLF transposing the PSD2 has approved a new and reformed legal framework for the majority of fintech companies currently operating in the Portuguese market, while simultaneously paving the way for new market players and new types of companies to enter the market and offer their products and services to both consumers and other businesses. It has also legally recognised third-party providers such as PISPs and AISPs, furthering the open banking ecosystem with the surging of new companies – such as payment initiation and account information services.

In parallel, crowdfunding investment schemes will also see an increase in both the number of entities operating in the market and the transaction volume associated with these types of investments, pursuing more democratic and decentralised equity and debt markets, as both the consumer market and the regulators themselves are beginning to be more aware and prone to the changes in the way some services are provided in the financial sector.

Regulation of the cryptocurrencies market has not yet been subject to public discussion or a more focused regulatory analysis by either the Bank of Portugal or the CMVM. Apart from some of the mentioned warnings issued by both entities, Portuguese regulators have adopted a ‘wait and see’ and case-by-case approach in this respect. As such, and despite the unpredictability of this issue – where opinions change and evolve at almost the same pace as the market itself – there is no envisaged change to the legal or regulatory status of cryptocurrencies other than the mentioned amendment to the AML Directive, which still has not been implemented into national law.

The Portuguese fintech market, which has observed a rather slow but steady development, shall greatly benefit from the PSD2 innovations in the areas of open banking and payment initiation services, with new players entering the market in this segment and new solutions being developed by traditional banks (mostly where account information services are concerned). These may provide an incentive for regulatory and supervision authorities to look into this ever-evolving market more closely, whether by fostering innovation by means
of friendlier regulation or by furthering the existing regulation into accommodating the new paradigm shift from traditional physical banking to an open and digital financial economy. Increasing the means of remote account opening, adapting the AML-related obligations to a digitalised reality, among others, may prove indispensable for the continuous evolution of the Portuguese fintech market.
I  OVERVIEW

Digital transformation greatly impacts the financial industry. Banks and other credit institutions in Russia know this first-hand, as they face greater competition and more demanding customers. This compels financial service providers to constantly experiment with new technologies and business models, thus paving the way for a growing interest in fintech. This makes particular sense when you consider how attractive the customer base is in Russia, where there are more than 146.7 million citizens and a high internet penetration rate of 76 per cent.

Overall, Russia can be categorised as a fintech-friendly jurisdiction with no unusually burdensome requirements on companies involved in this field of commerce. There are some obstacles and uncertainties that may impact certain business models, but we expect this to change soon because of recent efforts aimed to upgrade Russian regulatory framework for digital economy (see Sections VIII and IX for details).

The main regulator, the Central Bank of Russia (the Central Bank), also demonstrates an open-minded approach towards new financial technologies and maintains an informative website in English. Interested parties may engage with the regulator in several forums, such as Finopolis, an annual fintech conference organised by the Central Bank in Sochi, the Association for Financial Technologies Development and in various smaller working groups.

Big banks in Russia lead the innovation race by leveraging existing relationships and data about their customers. For example, the largest banks are building their own financial marketplaces and peer-to-peer lending platforms. However, there are also many smaller companies and start-ups trying to challenge incumbents, especially in such areas as point of sale technologies and payment solutions.

Supporting fintech companies with economic incentives would certainly help, as there are currently no specific tax incentives for fintech companies in Russia. Fintech start-ups, however, may take advantage of benefits available for IT companies, such as reduced social security contribution rates of 14 per cent on employees’ wages (instead of 30 per cent for other companies) or even more substantial tax privileges for residents of ‘technoparks’ (Skolkovo, for example).

1 Roman Buzko is a partner at Buzko Legal.
2 https://www.cbr.ru/eng/.
3 Information in English available at: https://finopolis.ru/en/.
II REGULATION

i Licensing and marketing

‘Fintech’ companies provide financial services using big data, artificial intelligence (AI), machine learning, robotisation, blockchain, cloud technologies, biometrics, etc. Thus, the business models range drastically from traditional payments and collective investments to such novel areas as cryptocurrencies, initial coin offerings (ICOs) and robo-advisers. Each business model is always subject to its specific set of regulations and licensing requirements.

Given this fact, there is no universal fintech licence in Russia. Instead, each business model of fintech is regulated separately. Some business models, such as payments, are subject to established regulations that were adopted several years ago, while many others are subject to no regulation at all or operate in the grey area of the law.

The main financial regulator is the Central Bank, which oversees the monetary policy and regulates the financial industry. The Central Bank is the main licensing authority for banks, insurance companies, broker-dealers, investment advisers, payment systems, etc.

Apart from the Central Bank, some other authorities have adjacent functions in the regulation of fintech:

- the Ministry of Finance is responsible for general financial policy and overall management in the field of finance in Russia;
- the Federal Tax Service is a part of the Ministry of Finance and supervises compliance with taxation rules, including taxation of cryptocurrency mining and transactions with cryptoassets;
- the Federal Financial Monitoring Service (Rosfinmonitoring) is mainly tasked with anti-money laundering (AML) and counter-terrorism financing functions; and
- the Federal Anti-Monopoly Service enforces regulations applicable to fair competition and advertising, including those related to financial products and services.

Despite the leading role of the Central Bank, with the adoption in 2015 of the Federal Law on Self-Regulated Organisations in Financial Markets,\(^5\) certain regulatory functions have been delegated to self-regulated organisations (SROs). As of February 2020, there are 24 SROs in the field of finance approved by the Central Bank. In addition to SROs, there are also industry organisations and unions active in the fintech area, such as the Association for Financial Technologies Development,\(^6\) launched by the Central Bank, and the Russian Association for Cryptocurrency and Blockchain.\(^7\)

In line with global practice, the Central Bank and other regulatory authorities in Russia place special emphasis on consumer protection. This is achieved through the enforcement of rules applicable to marketing and advertising of financial products. The principal source of such rules is the Federal Law on Advertising,\(^8\) which sets basic principles, bans misleading and unfair advertising practices and provides for specific rules applicable to financial services and securities. In addition to that, the Federal Law on Consumer Protection\(^9\) sets forth detailed rules aimed to protect consumers.

\(^6\) See footnote 4.
\(^7\) https://racib.com/.
\(^8\) Federal Law No. 38-FZ on Advertising dated 13 March 2006.
When it comes to competition, the main Act is the Federal Law on the Protection of Competition,\(^{10}\) which prohibits unfair competitive practices and outlaws abuses of dominant position, with special rules for financial organisations.

Since 2015, after the adoption of the Federal Law on Credit Histories,\(^{11}\) there is now a legal framework for credit information services provided by credit history bureaus. These are private companies providing information services about the creditworthiness of borrowers. Professional lenders are required to submit information about individual borrowers to at least one such credit history bureau. As of February 2020, there are 11 credit history bureaus registered with the Central Bank.

### ii Cross-border issues

Unlike in some other jurisdictions, regulated or licensed financial activities may not be passported from other countries into Russia (i.e., companies incorporated abroad and licensed or regulated under their local rules may not automatically become licensed or regulated in Russia). A certain level of passporting may become possible in the future among countries that are members of the Eurasian Economic Union (Armenia, Belarus, Kazakhstan, Kyrgyz Republic, Moldova, and Russia).

Traditional financial services that are subject to licensing or registration, such as banking, insurance, brokerage and dealing in securities, require a licence and may be carried out only via a local legal presence. Active targeting of Russian customers may result in liability and blocking of a perpetrator’s website in the territory of Russia. Certain industries are also protected against foreign competitors willing to enter the Russian market. For example, there is a 50 per cent quota on the aggregate amount of foreign capital for banking and insurance industries. Otherwise, there are no restrictions on foreign investors willing to explore fintech opportunities via a local legal presence; nor are there requirements to partner or engage with local companies to enter the Russian market.

There is a general rule that foreign organisations engaged in regulated activities on the securities market under their local laws may carry out such activities in the territory of Russia only subject to prior accreditation with the Central Bank. However, the accreditation guidance developed in 2015 has not yet been adopted, which makes this rule of little practical value.

Despite the lack of passporting and certain restrictions, many fintech services are offered to Russian customers from abroad. This is particularly the case for unregulated segments of fintech, such as cryptocurrencies and ICOs. By way of example, until 2015, the trading of foreign currencies, universally known as ‘forex’, was unregulated in Russia and was actively marketed by offshore companies to a Russian audience.

Besides unregulated business, there are also examples of foreign financial service providers being available to Russian consumers, without being legally present on the Russian market. This may be the case when a consumer only needs to be able to speak English to access a website where a fintech product is offered, whereas the website itself may not necessarily be actively marketed to the Russian audience. As an example, many foreign crowd-investing and automated investment adviser platforms are available to Russian consumers, even though they are likely offering regulated services. In the era when many financial services are offered

---

through desktop or smartphone application interfaces, one must take active steps to not to be present in a particular market, such as blocking by IP addresses, limiting traffic-generating campaigns to select areas or limiting incoming payments to certain banks.

III  DIGITAL IDENTITY AND ONBOARDING

Over the past couple of years, the Russian government has made significant efforts to introduce a digital identity for individuals and companies. This was initially driven by the desire to improve and ensure access to public services via the internet, which required a stable identity management system in place. Such a system, the Unified System of Identification and Authentication (USIA), was created in 2010 with a view to providing access to an online portal of public services, Gosuslugi. As of the beginning of 2018, more than 100 million Russian citizens are registered in the USIA.

Nowadays, the use of the USIA as a method of identification has been extended beyond public services. Certain financial service providers that were previously required by AML or KYC laws to identify clients in their presence may now use USIA as a gateway. For example, this applies to consumer (micro) loans, brokerage, securities trust management, and certain other financial services, thereby allowing full digital onboarding.

On 2 July 2018, the Unified Biometric System (UBS) was put into operation. UBS allows customers to undergo the biometric identification procedure. Customers need to visit one of the partner banks once, and can then use their unique biometrical profile to access financial products remotely. Since the end of 2019, UBS has been used to open bank accounts, obtain credit and carry out transactions in any bank. It is expected that UBS will be rolled out for other financial products, such as insurance and microfinancing, allowing for full digital onboarding.

IV  DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i  Digital marketplaces

Digital marketplaces correspond to platforms where entrepreneurs place commercial offers for an indefinite range of consumers, who then select goods that best suit their needs. Currently, special rules establishing procedures to monitor the operation of marketplaces are lacking. Each operator develops its own terms of service, to which sellers and consumers must adhere in accordance with the Article 428 of the Civil Code of the Russian Federation. It is often the case that marketplace operators fix their roles as aggregators and provide that they are not responsible for the quality, time limits and other parameters of sales of goods. However, the rights, obligations and responsibility of trade aggregators are still subject to the provisions of the Federal Law on the Protection of Consumers and the Federal Law on Personal Data.

In the short term, the Central Bank will also launch a marketplace operating in the sphere of financial transactions. The integral part of the marketplace’s system will be taken by electronic platforms, where financial service providers (credit and non-credit institutions, as well as securities issuers) put their offers of financial services for authorised consumers. Such platforms will be managed by providers, established under the Russian law and listed in

the Central Bank’s register. The future legislative framework for addressing this marketplace will be based on a special law. As of February 2020, relevant bills are at the initial stage of adoption in the State Duma of the Russian Federation.

ii Digital and cryptoassets
For the last two years, the legal framework for digital and cryptoassets has been actively developed. The provisions of the bill are generally accepted by the Ministry of Finance and other competent bodies. However, the Bank of Russia’s representatives expressed their concerns over the circulation of cryptocurrencies, as they pose a high risk of enabling the laundering of illegal funds.

Nevertheless, the Central Bank’s criticism relates only to certain aspects of the circulation of cryptocurrencies that are not backed by an underlying asset (e.g., as with stablecoins) or are not guaranteed by any state.

iii Collective investment schemes
There are several legal forms that can be used for collective investment purposes in Russia, ranging from purely contractual, such as ‘investment partnership agreements’, to corporate ones, such as joint stock companies or incorporated investment funds. At the same time, available legal forms are not very well suited for modern-day crowd-investing purposes. The main hurdles are high incorporation costs, restrictions on the transfer of investment interests or other burdensome requirements.

The standard choice for a large-scale collective investment scheme remains a ‘unit investment fund’. This legal form has been successfully used in the domain of collective real estate investments. The fund must be run by a professional investment management company.

Another option that is suitable for small-scale collective investments is a typical limited liability company (LLC). In this case, investment opportunities are marketed on an online platform, but actual transactions take place offline, since the transfer of interest in an LLC is subject to notary certification. The total number of members in the LLC is capped at 50.

iv Crowdfunding and crowd-lending
The law regulating crowdfunding and crowd-lending (or peer-to-peer lending) in Russia entered into force on 1 January 2020. Existing platforms must comply by 1 July 2020. The new law determines the definition of an investment platform; establishes requirements for operators (that must be included in the Central Bank’s register, prepare annual reports on the results of their activities and possess capital of no less than 5 million roubles), investors (for unqualified investors – no more than 600 000 roubles in a year) and persons attracting investments; and introduces restrictions on the total amount of investments (no more than 1 billion roubles in a year). It is worth mentioning that crowdfunding and crowd-lending activities in Russia are not subject to licensing or consumer lending regulations.

---

Despite the fact that the new law has finally provided for a legal framework in crowdfunding relations, it primarily focuses on protecting retail investors rather than simplifying the investment process and eliminating barriers. This may limit the potential for crowdfunding as an alternative to traditional sources of capital for businesses. Moreover, according to the Central Bank’s report, \(^\text{15}\) in the first three quarters of 2019 the Russian crowdfunding market decreased by more than 40 per cent (peer-to-peer lending suffered a decrease of 70 per cent, from 268 million to 80.6 million roubles). The reasons for the decrease are the active involvement of banks in the process and the decline in investors’ activities. However, experts predict the crowdfunding market’s recovery in 2020 thanks to the emergence of more than 10 new players, including Sberbank and Alfa-Bank.

\section*{v Payment services}

Payment services is a regulated activity in Russia. The main piece of legislation is the Federal Law on the National Payment System \(^\text{16}\) (the NPS Law), which is supplemented by numerous detailed regulations. The NPS Law describes different types of activities within the national payment ecosystem and imposes requirements depending on the type of activity. Credit institutions, including banks, may engage in most types of payment activities, whereas non-banking credit institutions are limited to certain activities (such as payment-clearing services and processing). As of February 2020, there were 51 active payment systems listed in the register maintained by the Central Bank. \(^\text{17}\)

Since 28 January 2019, following the Central Bank’s roadmap of 2018–2020, the Faster Payments System (FPS) along with the National Payment Card System are fully operated. As of February 2020, 44 banks are participating in the system. The FPS enables private consumers to make instant online payments 24/7 using simple identifiers (e.g., a mobile number, QR code) regardless of in which banks the senders or recipients have their accounts.

Notably, since the grace period of 2019, the FPS transfers between individuals are free of charge for banks, but from 30 June 2022 banks will have to pay rates. Nowadays, rates are established for funds transfers from legal entities to individuals, effective from 1 April 2020.

Since the adoption of several federal laws \(^\text{18}\) in 2019, there are other noteworthy developments concerning foreign payment systems (Visa, MasterCard, etc.) operating in Russia that prohibit foreign payment systems from refusing to provide services to Russian banks as of April 2020, and oblige them to create separate subdivisions in Russia and register with the Central Bank as of July 2020.

\section*{vi Open API}

Unlike the European Union, where PSD2 will oblige banks to provide access to their customers’ account information through application programming interfaces (API) to third parties, banks in Russia are not presently subject to such obligation. Nonetheless, the Central Bank expects a law establishing the obligation of open API for all banks to be adopted by the first quarter of 2021. \(^\text{19}\)

\begin{itemize}
\item \(^\text{15}\) https://www.rbc.ru/finances/18/11/2019/5dcd55c19a794751a1a5c3ca .
\item \(^\text{16}\) Federal Law No. 161-FZ on National Payment System dated 18 July 2011.
\item \(^\text{17}\) Available in Russian at: www.cbr.ru/PSystem/rops/ .
\item \(^\text{19}\) https://www.kommersant.ru/doc/4060395.
\end{itemize}
V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

As early as 2014, various regulators in Russia for the first time acknowledged the existence of Bitcoin by demonstrating their negative views towards it. In 2017, the attitude of regulators towards Bitcoin shifted from ‘banned, unrecommended’ to ‘the concept is under investigation, regulation will come soon.’

Regarding tokens and ICOs, it should be noted that since 1 October 2019 under Russian law tokens are legalised as objects of civil rights and are considered ‘digital rights’.20 Furthermore, the draft bill on digital financial assets is expected to outline the legal framework for blockchain (‘distributed registry system’), tokens and cryptocurrencies (‘digital currency’).

In its current form, the bill provides for ‘digital financial assets’ to be determined as ‘digital rights, including monetary claims, the possibility of exercising rights on equity securities, the right to demand the transfer of equity securities […] issuing, accounting and circulation of which is possible only by registering (changing) entries in the information system based on a distributed registry’. It means that security tokens (both shares tokens and tokenised securities) deriving their value from real assets (e.g., gold or nickel) could be considered ‘digital financial assets’ and will receive legal status after the adoption of the bill. For reference, utility tokens will also be legalised as ‘digital operation signs’ defined as ‘a set of electronic data (digital code or symbols) obtained by the rules of information systems, within which digital financial assets are issued. Such ‘digital operation signs’ fall out of the ‘digital financial assets’ definition. Their issuing and usage will be determined by the Central Bank. In this context, experts tend to agree that all tokens are different and thus should be treated according to their substance rather than form.

Internationally, one of the most widely discussed legal aspects of token sales was whether tokens constitute securities. Following the report of the US Securities and Exchange Commission on the DAO project,21 many regulators all over the world agreed that certain tokens may qualify as securities or other financial instruments. In Russia, the Central Bank has not taken a position on this issue yet. In fact, it is problematic to qualify a token as a ‘security’ under Russian law, since the Civil Code defines security by listing specific financial instruments in an exhaustive manner. Thus, unless specifically listed in Article 142, other instruments should not be considered securities. This approach contrasts with that in the United States, where courts lean towards a more flexible approach using the Howey test.

Russian securities law limits the circulation of foreign financial instruments, with the Central Bank having a final say on whether a particular instrument may be allowed to the public market. Unless cleared by the Central Bank, foreign securities may only be offered to accredited investors in Russia and no general solicitation is permitted.

AML and KYC rules apply to transactions with cryptocurrencies to the extent such transactions are carried out via ‘organisations carrying out transactions with monetary funds and other property’ as defined in Article 6 of the Federal Law on Combating Legalisation (Laundering) of Illegally Gained Income and Financing of Terrorism.22

VI OTHER NEW BUSINESS MODELS

New business models in the area of fintech appear every now and then. Most of the time such models are beyond existing regulations and fall in one of the following two groups:

a. unregulated models, which may be implemented within the existing legal framework; and

b. prohibited models, which are explicitly outlawed.

Most new models fall within the unregulated domain. We will briefly cover several such business models below.

i Smart or self-executing contracts

Until recently, there was no specific mention of smart contracts in Russian law. As of October 2019, Article 309 of the Civil Code provides that ‘within the occurrence of certain circumstances legal transaction may be executed without additionally expressed will of its parties by applying information technologies under the terms of transaction’.

Certification of Masterchain, an Ethereum-based blockchain developed by the consortium of major Russian banks cooperating within the Association for Financial Technologies Development, was made on 7 October 2019 demonstrates the readiness of blockchain technology (and smart contracts, in particular) to be used in the financial sector. Its White Paper names several use cases, such as a decentralised depository of mortgages, a distributed ledger of digital bank guarantees and electronic letters of credit.23

ii Automated digital advisery

Since 21 December 2018, automated digital advisory services (robo-advisers) have been subject to regulation. Specifically, Article of 6.2 of the Federal Law on Securities Market imposes mandatory accreditation for software used to provide investment advice. However, at this stage, the Central Bank has not yet adopted the procedure for such accreditation and, accordingly, no robo-advisers have been accredited.

iii AI

Currently, there are no special rules applicable to the use of AI in financial products. However, this does not preclude it from being actively developed. In early November 2019, Sberbank, Gazprom Neft, Yandex, Mail.ru Group, MTS and Russian Direct Investment Fund created the Russian AI Alliance. The parties joined forces to create technological components that will stimulate the development of AI. Thus, there is a great driver to develop legal regulations for AI in finance.

iv Financial product comparison

No specific regulation applies to websites comparing financial products or services. Such websites are nonetheless subject to general advertising and fair competition principles.

23 Masterchain’s whitepaper is available in English at: http://fintechru.org/documents/Masterchain_whitepaper_v1.1_en.pdf.
v Binary options
The Central Bank has not yet taken any stance on binary options. However, it did announce in its regulatory strategy for 2016–2018 that it would provide guidance on this issue. This announcement was made in the document’s section related to consumer protection and gambling.

VII INTELLIGENCE PROPERTY AND DATA PROTECTION

i Intellectual property
Russian law is familiar with all standard concepts of intellectual property (IP) used to protect business. Most commonly used are:

- patents (protecting inventions, utility models and industrial designs);
- trade secrets;
- copyright; and
- trademarks, including service marks.

Information of any nature relating to the results of intellectual activity may be treated as a trade secret and be protected as IP provided basic confidentiality conditions are met.

Software and databases are usually protected under copyright laws. Copyright is acquired automatically as of the date a copyright object is manifested in objective form. Registration is optional.

Rights over trademarks are granted by virtue of registration with Rospatent, a local patent and trademark office. Alternatively, rights may also be acquired by virtue of international agreements to which Russia is a party, such as the Madrid Convention. Russia is a ‘first-to-file’ jurisdiction.

Any foreign company may seek protection of its intellectual property in Russia provided national law requirements are met. Russia is also a signatory to most international treaties covering intellectual property protection.

Disputes often arise in the context of employment relationship as to who owns newly created IP. For an employer to acquire rights over such IP, it is important that an employment contract or a job assignment explicitly states that the creation of IP falls within the duties of an employee.

ii Data protection
Overall, Russian data protection law is in line with international standards. The Strasbourg Convention 1981 (ratified by Russia in 2005) laid the foundation for the Russian personal data protection legislation, which was adopted in 2006.

The main pieces of legislation governing the collection, storage and use of personal data in Russia are the Federal Law on Personal Data and the Federal Law on Information, Information Technologies, and Data Protection.
Unlike in some other jurisdictions, there is currently no general obligation to report cybercrimes, although such legislation was proposed in 2017 and may be adopted soon.

VIII YEAR IN REVIEW

The fintech agenda in Russia in the context of the Central Bank’s implementation of the Guidelines for Financial Technology Development for 2018–2020 was primarily focused on developing the legal framework for the digital era of finance. Specifically, the Bank of Russia has launched the regulatory sandbox as an isolated environment for piloting and modelling processes of new financial services, requiring changes in legal regulation. As of February 2020, the use of digital financial assets and biometric technologies, implementation of digital technologies in customer service processes and peer-to-peer insurance services are being successfully piloted in this regulatory sandbox.

Other than those specified in Sections III-VI, significant developments in the regulation and legal treatment of fintech include updates to the consumer lending legal framework, effective from 1 October 2019. Relevant changes cover remote customer identification for microcredit companies. Prior to that, all MFOs had to either delegate the simplified identification of customers to credit organisations (banks) or use the unified identification and authentication system (UIAS).

All recent developments are in line with the internationally accepted trends of the digitalisation of financial technologies.

IX OUTLOOK AND CONCLUSIONS

We expect the plans following the general trends of 2018 to be finalised in 2020. Specifically, we believe that the current trends will continue to evolve in 2020, with market participants focusing more on decentralisation and availability of market instruments for individuals and businesses.

Further, we predict that current global trends on RegTech (regulatory technology) and SupTech (supervision technology) development will continue to evolve in Russia. Basic business models have already been developed, and regulators need to understand how to control them. Financial institutions will continue to use innovations in order to comply with the regulator’s requirements, and regulators will implement Big Data, machine learning, AI, etc. to conduct effective supervision.


© 2020 Law Business Research Ltd
Chapter 19

SAUDI ARABIA

Suhaib Adli Hammad

I OVERVIEW

The boom of financial technology (fintech) in Saudi Arabia has led the Saudi Arabian Monetary Authority (SAMA) and the Capital Market Authority (CMA) to introduce new programmes to regulate the entities wishing to carry out fintech-related activities. In its efforts to contribute to Saudi Arabia’s Vision 2030 and diversify the economy, SAMA announced its acceptance of applications to its sandbox programmes starting from January 2018 to focus on the digitalised market Saudi Arabia is shifting towards. For fintech companies to enter the market in Saudi Arabia, they will be required to obtain the necessary licences from SAMA, the CMA or both, depending on the activities the fintech company wishes to carry out. These licences are merely temporary and in the form of letter allowing the accepted entities to engage in fintech-related activities for a trial period until being approved by the relevant authority.

Despite the fact that there have not been changes in the laws to fit fintech companies’ purposes, both SAMA and the CMA grant temporary experimental licences as an initiative to encourage the growth of fintech in Saudi Arabia. These licences are issued through an application to the relevant entity’s sandbox programme, but are still governed by the same laws which govern conventional financial transactions, which are as follows:

\begin{itemize}
  \item[a] general banking control laws;
  \item[b] general finance company control laws;
  \item[c] the E-banking Rules; and
  \item[d] the Electronic Transactions Law.
\end{itemize}

To further demonstrate Saudi Arabia’s initiative to cope with the digital market, a fintech guide was issued in February 2019 by Fintech Saudi highlighting the regulations governing the industry, the framework of their application and the options available for foreign investors to enter the Saudi fintech market. An updated version was published in July 2019. The release of a new version so soon after the original indicates that changes are happening rapidly in Saudi Arabian fintech law and that the country is paying close attention to the growth of fintech.

---

1 Suhaib Adli Hammad is a partner at Hammad and Al-Mehdar.
2 Check the activities listed by both to understand the relevant authority and seek the necessary license.
3 Fintech Saudi is a body that supports fintech companies by publishing guidelines to assist in understanding the framework available in Saudi Arabia. It is important to note that Fintech Saudi is not the body responsible for developing these regulations, but both SAMA and the CMA are strategic partners of Fintech Saudi.
This is also evidenced through the introduction of Fintech Saudi and its regular updates on the new laws and activities issued regarding the formation and regulation of fintech companies.

Furthermore, Fintech Saudi recently issued its 2019 report, which serves as a summary of the fintech ecosystem in Saudi Arabia while highlighting the developments undertaken by the relevant authorities to regulate the fintech boom in Saudi Arabia. The report further states that the governor of SAMA along with the governor of the CMA have been recently working on establishing the Fintech Saudi Hub, which will provide co-working spaces for entrepreneurs with fintech innovations while also hosting events and lectures related to the fintech field.

Since fintech transactions are still governed by conventional financial transactions laws, there are no specific tax regulations that apply to fintech companies. The General Authority of Zakat and Tax generally applies zakat on local companies and tax on foreign companies. The zakat is calculated to be 2.5 per cent of the capital of the company, while the tax on foreign companies or foreign shareholders in a company is usually 20 per cent of the revenue of the company, as opposed to the capital. Thus, fintech companies will be required to pay the same amounts based on the shareholders’ nationality. We believe that applying only a 2.5 per cent on local companies’ capital and 20 per cent on foreign shareholders’ revenue demonstrates the way in which tax laws in Saudi Arabia are company-friendly, which in fact means that they are fintech-friendly as well.

II REGULATION

i Licensing and marketing

Generally speaking, there have not been any alterations in the laws governing fintech as opposed to conventional financial transactions. Accordingly, all financial transactions are governed by the same laws, whether fintech or conventional.

Nevertheless, the relevant authorities are attempting to introduce fintech regulations to keep pace with the developments in Saudi Arabia. In the meantime, these are the options available for fintech companies to enter the Saudi market:

a alter the business carried out by the company to one that does not require SAMA or CMA licensing,
b partner with a local entity licensed by the relevant authorities; or
c enter the sandbox programmes offered by SAMA and the CMA that grant temporary or experimental licences. Fintech companies that carry out activities licensed by SAMA will have up to six months, subject to renewal, to practise their activities in the Saudi market. Companies that carry out activities regulated by the CMA will be given the opportunity to conduct business for up to two years and they may renew this licence once.

The temporary licence is a letter from the relevant authority allowing the specific company to practise its activities in Saudi Arabia while being monitored by such authority. A letter is only granted upon SAMA or the CMA’s acceptance of the application submitted by the entity. The application form is offered on SAMA/CMA’s website to provide clarity with regard to

---

4 You can find the application form by clicking the ‘Fintech Application’ button provided on this link: https://cma.org.sa/en/Market/Fintech/Pages/Default.aspx.
what is expected from the applicants. Upon CMA/SAMA’s acceptance of the application, the trial period shall commence, granting the entity the right to enter the Saudi market while carrying out its fintech activities. Once the licensed entity successfully completes its trial period, SAMA or the CMA will consider licensing the entity permanently. While there are 19 companies to date in the SAMA sandbox programme, on 2 February 2020, Menabytes, which covers technology and digital stories from the Middle East and North Africa, announced that two companies have been issued fintech licences by SAMA for the first time in Saudi Arabia upon successful completion of the SAMA sandbox trial period. STC Pay and Geidea, both offering payment fintech services, are now the first two companies to graduate from the SAMA sandbox programme and obtain a fintech licence.

In addition to granting temporary licences to practice fintech activities, SAMA and the CMA aim to regulate fintech in Saudi Arabia as follows. The CMA is the financial regulatory authority responsible for overseeing securities activities and crowdfunding solutions. SAMA, established by two royal decrees, is a regulatory, legislative and judicial body. Its legislative features emphasise, first, its responsibility for drafting and approving the laws on financial transactions – for instance, it approved the Charter of the Saudi Arabian Monetary Authority. Second, its regulatory element gives SAMA the authority to oversee and license entities that carry out financial activities. Finally, its judiciary feature allows for SAMA to establish its own judicial body to assume jurisdiction over claims related to financial activities such as e-wallets, payment mechanisms to validate e-signatures and e-transactions.

Fintech Saudi identified seven activities that do not require licensing by either SAMA or the CMA. These are:

- a) aggregation of publicly available financial information;
- b) business tools;
- c) back-office bank operations;
- d) enhancing bank’s customer experience;
- e) personal management;
- f) regulation technology (regtech), which involves the use of technology to support financial organisations to comply with financial services regulations. Fintechs can develop regtech solutions that do not conduct regulated activities but support financial organisations to remain compliant; and
- g) gamification.

Thus, carrying out such activities shall not trigger the application of the requirements to be licensed by the CMA or SAMA. Moreover, credit information services, falling under back-office bank operations, shall also be exempted from the requirement to be licensed since they are one of the seven activities that can be carried out with a licence.

Setting up an asset management company in Saudi Arabia is subject to licensing by the CMA as set out in the latter’s Investment Fund Regulations and Authorised Persons Regulations. This means that the entity must satisfy a number of requirements, such as

---

5 MB staff, STC Pay and Geidea Become First Two Companies to Get Fintech License from SAMA, February 2020.
a minimum capital requirement and establishing multiple internal key functions and appointing the required specialised officers, before being able to carry out its activities in Saudi Arabia.

Marketing and advertising of banking and financial services in Saudi Arabia are subject to the Banking Consumer Protection Principles issued by SAMA in June 2013. It is important to note that these principles govern and control only the content of the marketing material to be advertised by the financial institution.

Marketing is generally regulated by the Ministry of Culture and Information (MCI). The MCI obliges entities wishing to carry out advertising activities whether in print or electronically to obtain a licence, whether the entity is local or foreign. In accordance with MCI laws, the entity shall obtain a licence to be able to market its activities. Upon obtaining the relevant licence, the entity must comply with the banking Consumer Protection Principles with regard to the content of the material it desires to advertise.

It is important to note that these principles are applicable to financial institutions, and since Saudi Arabia remains silent with regard to the introduction of any special marketing laws applicable to fintech services, we believe that the same laws and principles will likely govern the marketing of fintech services in Saudi Arabia.

ii Cross-border issues

Activities that are regulated or licensed by a foreign jurisdiction cannot be passported to Saudi Arabia's jurisdiction. For a foreign company to carry out its activities in Saudi Arabia, it must have local legal presence in Saudi Arabia subject to local licensing. Hence, the company from another jurisdiction will be required to seek the relevant licensing in Saudi Arabia depending on its activities from SAMA, the CMA or both, and from the Ministry of Investment (MISA).

If the foreign entity attempts to undertake its activities in Saudi Arabia without legal presence in Saudi Arabia, the transfer of monetary amounts from the local account to the foreign account may trigger a red flag with the banks, which may subject the entity to investigation. To avoid this, the foreign entity should have a local bank account and opening a local bank account entails having a local presence.

Cross-border services or products cannot be offered without a local presence. Hence, the fintech service or product can be offered in Saudi Arabia once the company offering the service or product establishes local presence either by establishing a new company and obtaining a MISA licence or, in limited instances, appointing a Saudi-licensed agent in Saudi Arabia to provide the services or products on their behalf.

Marketing is subject to specific licensing, whether carried out by a local or foreign entity. Accordingly, if the foreign entity wishes to appoint a local entity to solicit the services, it shall ensure that the local entity is licensed by the MCI to carry out marketing and advertisement activities provided that such advertisement is in line with the Banking Consumer Protection Principles issued by SAMA. The only difference between appointing a local partner and actively marketing is where the entity chooses the option to appoint a partner to solicit the service; this will exempt that entity from seeking the necessary marketing licence provided that the local partner is licensed by the relevant authorities. Owing to the importance of the licensing requirement, we usually ask foreign entities to conduct licensing related due diligence before deciding to appoint a local partner.
First, regarding foreign exchange or currency control, in order for an entity to open a bank account in Saudi Arabia it must establish legal local existence, which subjects it to MISA licensing. Also, if it is seeking local existence then opening a bank account in Saudi Arabia is required.

Once an entity has successfully established itself in Saudi Arabia and has opened a local bank account, the transfer of the amounts collected in Saudi Arabia to the parent company’s offshore account will be permissible.

Furthermore, with regard to cryptocurrencies specifically, despite its warning about transacting with the cryptocurrencies that are in existence today, SAMA has been experimenting with the United Arab Emirates’ (UAE) Central Bank blockchain cross-border transfers and payments in its efforts to issue its own digital currency to be used in cross-border transactions. Moreover, the Saudi Central Bank has contracted with US-based Ripple to introduce pilot programmes for Saudi banks. This programme attempts to radically shift the banking system in Saudi Arabia by allowing transactions in digital currencies. At the Financial Sector Conference in April 2019, Saudi British Bank (SABB) stated that it will launch its Ripple-based cross-border payments through blockchain. Accordingly, Saudi Arabia’s efforts to introduce its own digital currencies are evident through its contracts with the UAE’s Central Bank and US-based Ripple.

To contribute to diversifying the economy in support of Saudi Arabia’s Vision 2030, MISA minimised its requirements for foreigners to obtain the necessary licences to establish entities in Saudi Arabia. Thus, for foreign persons to enjoy the right of ownership in Saudi Arabia, they will be subject to MISA licensing based on the activities they wish to carry out. It is important to note, however, that there are some activities that may not be carried out by foreigners as per MISA’s list of activities that are restricted for foreign visitors. In addition, some activities may entail the satisfaction of certain requirements or partnering with a local shareholder. These requirements differ based on the activities carried out by the company to be established in Saudi Arabia. The foreign entity has four available options to carry out its activity in Saudi Arabia. It may:

- establish a subsidiary of an existing foreign company by obtaining the relevant MISA licence;
- start a new fintech company through MISA’s entrepreneurial licence;
- license the fintech company to a Saudi start-up; or
- appoint a sales agent in Saudi Arabia.

III DIGITAL IDENTITY AND ONBOARDING

The only digital identity available in Saudi Arabia is issued by the state and is only offered for the government sector. Each citizen shall have his or her identity registered with Saudi Arabia’s Ministry of Interior (MOI) by registering their fingerprints and creating an ABSHR

---

9 Arab News; What is Blockchain, and Why Do the UAE and Saudi Arabia Want to Use it.
11 SABB website.
account. Upon registering with the MOI, a number of government services can be provided using the digital identity, such as the issuance of powers of attorney, and the issuance and payment of traffic fines.

The registration of ABSHR accounts is only available for residents of Saudi Arabia, whether they are nationals or not. Nationals will register electronically using their national ID numbers, then activate the account by registering their fingerprints on machines offered in a number of locations in Saudi Arabia (mainly in malls for ease of access). Non-national residents, on the other hand, register electronically using their ‘iqama’ number, then register their fingerprints in the same manner nationals do for activation of account. Upon successful activation, residents of Saudi Arabia will be able to enjoy the services offered by the MOI electronically.

As mentioned above, digital identity is only provided for the government sector. We still do not see it being applicable to financial services, but we believe it may be introduced in the next couple of months, with SABB attempting to offer cross-border blockchain transactions, as mentioned earlier.

IV  DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

Collective investment, governed by SAMA, is generally allowed but subject to licensing and minimum capital requirements. Any activity with the purpose of financing is regulated by the Finance Companies Control Law promulgated by Royal Decree No. M/51 dated 13/08/1433 H (corresponding to 02/07/2012 G) (the Finance Companies Law) and its Implementing Regulations. Since the purpose of collective investment is to finance companies, it will trigger the application of the Finance Companies Law. As per the Finance Companies Law and its implementing regulations, financing activities may not be carried out in Saudi Arabia without obtaining the necessary licences from SAMA, provided that such activities are in compliance with shariah principles. Thus, any entity desiring to manage investments for the purpose of financing other entities will be subject to SAMA licensing requirements.

To be able to create a portal to regulate collective investments, the entity that is the manager of the investment shall seek to obtain the necessary licence offered by SAMA. Furthermore, since such activity may trigger money laundering risks, being the manager of such investment may be subject to investigation. As a result of these risks, SAMA is reluctant to allow individuals or entities to collect amounts, fearing that they may be used for wrongful purposes unless they can demonstrate sufficient evidence of how they intend to monitor closely every transaction made. Hence, to obtain the necessary licensing, we advise the entity to consider how to mitigate any money laundering-related risks and communicate these considerations to SAMA.

The CMA allows for equity-based crowdfunding in Saudi Arabia, subject to regulation by CMA laws and regulations. The entity shall first apply via the CMA’s portal to obtain a temporary licence to carry out crowdfunding activities during a trial period. Similar to collective investment, because money collection is a sensitive activity, it is important to note that the entity wishing to crowdfund must provide sufficient evidence of how it intends to monitor closely any money laundering activities that may occur. Upon the entity’s acceptance by the CMA and successful completion of the trial period, it may be granted a permanent licence allowing the entity to carry out crowdfunding activities in Saudi Arabia.

Similar to collective investment, since peer-to-peer lending falls under financing activities, it shall be governed by SAMA and subject to the Finance Companies Law. In
order for an entity to carry out the activities related to peer-to-peer lending, it shall ensure that its entity is licensed by SAMA and that the activities being conducted are in line with shariah principles.

Furthermore, it is important to note that where the entity is responsible for managing the amounts, it will be subject to CMA regulations. This is because management activities fall under Securities Business activities as listed in the Securities Business Regulation issued by the CMA. Thus, due to peer-to-peer lending being a financial activity and its management falling under Security Business activities, such entity will trigger SAMA and CMA licensing requirements. Once all licences are obtained, the entity will be authorised to carry out lending and management activities in Saudi Arabia.

We are not aware of such activities yet being carried out in Saudi Arabia nor of the way in which the laws would govern such trading.

Payment services in Saudi Arabia will trigger the application of the Banking Control Law which applies to banks generally. Thus, any payment services activities will require licensing by SAMA (i.e., PayPall, HyperPay and PayTab). Accordingly, where an entity desires to carry out payment services, it must obtain the necessary licences from SAMA, partner with an entity licensed by SAMA, or appoint a local agent licensed by SAMA and licence the local agent to carry out the payment services activities.

With regard to making client data accessible to third parties, there are no laws mandating that clients’ information be kept confidential. However, it is common practice to keep such information confidential, especially with the introduction of the E-Commerce Law in July 2019 and its implementing regulations earlier this year. The E-Commerce Law is the first law to put an obligation on entities to keep its clients and users’ information confidential when transacting electronically. Based on this provision, we believe Saudi Arabia is moving towards imposing a legal duty on entities to keep clients’ information confidential and making this a legal obligation subject to sanctions in case of violation.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

Despite SAMA’s warning on transacting with cryptocurrencies in existence today, it has been experimenting with the UAE Central Bank and US-based company Ripple to introduce blockchain cross-border transfers and payments while considering whether to issue their own digital currency. However, there are no special laws governing blockchain technology yet, so it remains subject to conventional financial transactions laws.

There are no legal standards governing blockchain and cryptocurrencies so far. Therefore, the laws are unclear with regard to the qualification of tokens as securities. We do believe that money laundering rules and tax laws will be applied to new technology in a similar way to conventional financial transactions.

VI OTHER NEW BUSINESS MODELS

There are no laws governing the permissibility of self-executed contracts yet. However, contracts in general are governed by shariah principles in Saudi Arabia. As long as an offer, acceptance and consideration are demonstrated, a contract shall be held valid under shariah principles. Hence, we believe that if smart contracts follow the same process, they shall be admissible in Saudi Arabia.
With regard to arbitration, we believe the same arbitration laws governing conventional contracts shall be enforceable on self-executed contracts. This is because Saudi Arabia’s laws of arbitration apply to any arbitration, regardless of the nature of the legal relationship between the parties in dispute.\textsuperscript{12}

As discussed above, automated processes are not yet permitted. Nevertheless, we presume that if it is executed in a manner that complies with shariah principles then it shall be permitted.

Third-party websites comparing products or providing information about financial products are subject to SAMA regulations. Such websites are currently considered brokers by SAMA and are therefore subject to licensing requirements to enter into its sandbox programme.

Saudi Arabia has recently been developing new laws in its efforts to address the changes following Crown Prince Mohammed Bin Salman’s Vision 2030. However, there are still no specific laws regulating fintech in Saudi Arabia. Nevertheless, with Saudi Arabia undertaking rapid changes to diversify the economy and the flourishing of fintech-related activities and companies in Saudi Arabia, we expect new regulations to be developed and new laws introduced that are tailored to fit the industry. Furthermore, we believe that establishing an entity responsible for regulating the new developments in fintech is a strong indicator that Saudi is monitoring the growth in fintech and is preparing a targeted response.

\section*{VII INTELLECTUAL PROPERTY AND DATA PROTECTION}

There are four means of protecting intellectual property:

\begin{itemize}
  \item[a] trademark registration;
  \item[b] patent registration;
  \item[c] industrial designs registration; and
  \item[d] copyright.
\end{itemize}

Trademarks are registered through the Ministry of Commerce’s (MOCI) portal where the applicant may register the name and logo of his or her entity. Industrial designs may also be registered through the MOCI. Patents, on the other hand, are protected by registration with either the King Abdulaziz University for Science and Technology (KAUST), where KAUST will be entitled to a percentage of the patent to be registered, or the King Abdulaziz City for Science and Technology (KACST), though the process is lengthy and complex.

Based on the above, the options available for IP registration and protection in Saudi Arabia, are, generally speaking, difficult to implement in practice. Due to the complexity of the process, clients usually resolve to protect their rights via registering them in the United States then equalising the certificate to be used in Saudi Arabia. This is the case for patents, too.

In order for software to be protected, its code shall be revealed in detail for copyright purposes since codes cannot be patented. Upon revealing the code of the software, it will be subject to copyright laws, since copyright in Saudi Arabia is protected for 50 years after publication, subject to renewal. Owing to the level of exposure this process entails, this mechanism is not that preferred by software owners. Thus, we advise software owners wishing to protect their software to register the software’s trademark for protection, since the software itself cannot be protected.

\textsuperscript{12} Article 2 of the Law of Arbitration of Saudi Arabia.
Where an employee develops software, its ownership rights merely depend on the contract between the employee and his/her company. There are no specific laws governing this matter.

As mentioned above, the first law enforcing an obligation on entities to keep their clients’ or users’ information confidential was introduced in July 2019. The E-Commerce Law\textsuperscript{13} demonstrates Saudi Arabia’s attempts to highlight the importance of keeping clients’ data safe. Hence, despite the fact that there are no laws imposing a legal duty on entities to keep their clients’ data confidential, we believe that the E-Commerce Law and its implementing regulations will set a threshold to be met by entities to ensure their clients’ data is protected. Based on that, we also believe new laws may be introduced on data protection and old laws amended to impose duties on parties to protect the confidentiality of individuals’ data and information.

\section*{VIII YEAR IN REVIEW}

With the growth of fintech in Saudi Arabia, SAMA and the CMA’s efforts to support the industry can be clearly demonstrated through the number of experimental and permanent licences they have granted to fintech companies during the last three years. Accordingly, despite the fact that there are no developments in the legal treatment of fintech companies and new regulations governing this type of companies have not yet been introduced, the CMA and SAMA have accommodate the fintech market’s needs by allowing more companies to carry out fintech activities through their sandbox programmes and by granting licences for fintech activities. SAMA has gone so far as to grant two entities a permanent licence upon the successful completion of their trial period. Based on this initiative by SAMA and the CMA, and their close monitoring process during the trial period, we believe Saudi Arabia may introduce new laws to accommodate the market’s needs in the near future.

\section*{IX OUTLOOK AND CONCLUSIONS}

The Saudi market is adapting quickly to global market trends and innovation is occurring faster than the legislation regulating it. SAMA and the CMA are still examining the fintech companies operating within their sandbox and experimental programmes very closely. They are continuing to regulate the operation of fintech companies through existing legislation, which was not drafted with the introduction of technology to the financial sector in mind. While their efforts to support the ecosystem are commendable, the current regulations should be updated and new guidelines developed on licensing and operating fintech companies with new concepts such as crowdfunding, robo-advice and micro-lending.

\textsuperscript{13} Approved on 9 July 2019 pursuant to Royal Decree No. M/126.
Chapter 20

SINGAPORE

Adrian Ang V-Meng and Alexander Yap Wei-Ming

I OVERVIEW

The Singapore government and related statutory boards have identified fintech as a growth area for the Singapore economy. Following on from this, a not insignificant amount of resources have been channelled into the space. By way of example, the Monetary Authority of Singapore (MAS) has formed a Financial Technology and Innovation Group to drive fintech initiatives, with divisions specifically responsible for developing the Singapore payments ecosystem and cross-border data connectivity, scanning the horizon for cutting-edge technologies with potential financial industry application, and developing and implementing AI strategy for the Singapore financial industry. In addition, Singapore offers an open banking platform via application programming interfaces for faster innovation and integration of new and legacy IT systems within the sector. MAS also launched two ‘sandboxes’ as safe spaces for fintech companies to experiment and roll out innovative products and solutions within controlled boundaries.

In conjunction with the above, there are several schemes aimed at supporting fintech innovation such as:

- the Technology Enterprise Commercialisation Scheme;
- the Financial Sector Technology and Innovation (FSTI) scheme; and
- the Capabilities Development Grant – Technology Innovation.

For the FSTI scheme, which is intended to support the creation of a vibrant ecosystem for innovation, MAS has committed S$225 million over a five-year period to help financial institutions set up innovation labs in Singapore, fund technology infrastructure to deliver fintech services, and provide support for early-stage development of innovative projects through the FSTI proof of concept initiative.

There are several additional grants, schemes and initiatives which aim to facilitate access to capital for fintech entities in Singapore. These include:

- A.I.SG is a national programme which is expected to involve investment of S$150 million over five years to boost Singapore's artificial intelligence (AI) capabilities.
- The Accelerated Initiative for Artificial Intelligence was recently commenced in April 2019 by the Intellectual Property Office of Singapore (IPOS) to accelerate grants of AI-related patent applications to just six months, compared to a typical period of at
least two years or more. This initiative is also available to AI innovators (both individuals and corporate entities) outside of Singapore, allowing them to use Singapore as a base to access markets of their interest speedily.

c Accreditation@SGD is a programme through which the Info-Communications Media Development Authority will accredit promising technology product firms, in order to help them establish their credentials and position them as qualified parties to potential buyers and customers. This involves an independent evaluation of the technology product firms on the basis of various factors, including whether their products function in accordance with stated claims.

d Startup SG Accelerator, Startup SG Equity, Startup SG Founder and Startup SG Talent (all operated by Enterprise Singapore), are schemes which provide the Singapore tech start-up ecosystem with government co-investment, mentorship support and start-up capital grants. For example, Startup SG Talent aims to foster a more conducive environment for promising global talent to set up innovative businesses in Singapore and for start-ups to attract global talent to become part of their team (including in particular the EntrePass scheme, which allows eligible foreigners to start and operate a new business in Singapore).

e The Enterprise Development Grant is managed by Enterprise Singapore and is designed to help companies in Singapore build internal capabilities. Under this programme, Singapore companies (with at least 30 per cent local shareholding) may obtain government grants of up to 70 per cent of the qualifying product costs for upgrading initiatives in areas such as increasing productivity, process improvement, product development and market access.

f The Early Stage Venture Fund, an initiative under the National Framework for Innovation and Enterprise, through which the National Research Foundation Singapore invests SG$10 million on a matching basis to seed corporate venture capital funds to invest in Singapore-based early-stage technology start-ups.

II REGULATION

i Licensing and marketing

Fintech-related legal work regularly covers a broad range of topics and typical topics include:

a financial regulatory and compliance (e.g., the type of licence that will need to be issued by the relevant authority or licensing exemptions that may be applicable to a fintech product or service);

b technology contracts (e.g., software licensing contracts or terms of use of the fintech product or service);

c data protection (e.g., the obligations imposed on fintech companies in relation to personal data or personally identifiable information that they may handle);

d intellectual property issues (e.g., intellectual property protection and management); and

e financings (e.g., venture capital investments in fintech companies).

A fintech company should consider whether a licence from a regulatory authority is required (i.e., regulatory licensing issues) as a priority. This is to reduce the risk of a potential licence application procedure holding back the roll-out of a fintech product or service. Fintech products and services come in a variety of forms and there is no one ‘fintech licence’ that
applies to all fintech products and services. Different pieces of legislation may apply to different fintech products and services depending on the scope of the product or service being offered. The specific regulatory authority that regulates the activities of the fintech product or service will vary depending on the scope of such product or service. From experience, the regulatory authorities that oversee fintech-related activities will typically be MAS, the Registry of Moneylenders and Enterprise Singapore.

If the fintech product or service requires a licence from an authority, it will likely take months before a particular licence is issued. The speed of the grant of a licence will depend (among other things) on the quality and completeness of the application and the level of regulatory comfort that the fintech company provides to the authority. The authority will typically require some time to consider the details of the licence application and the fintech company may also need some time to respond to questions from the authority on the specifics of the product or service.

Depending on the specific scope of activities of the fintech product or service, the following (non-exhaustive) issues may need to be considered:

- **a** licensing requirements for regulated activities under the Securities and Futures Act (SFA) (e.g., ‘dealing in capital markets products’ and ‘fund management’);
- **b** prospectus requirements for the offer of securities to persons in Singapore under the SFA;
- **c** licensing requirements for regulated activities under the Financial Advisors Act (FAA) (e.g., providing financial advisory services);
- **d** licensing requirements for moneylending under the Moneylenders Act;
- **e** licensing requirements for providing payment services under the Payment Services Act; and
- **f** regulatory requirements imposed on the operator of a ‘payment system’ under the Payment Services Act.

Prior to undertaking any marketing of a fintech product or service, a fintech company should determine if it is undertaking a regulated activity and whether a licence is required for it to operate. There may be restrictions as to the scope of marketing activities that a fintech company can undertake and this will typically revolve around the issue of whether (and how) the activities of the fintech company is regulated. For example, a fintech company that operates a securities crowdfunding platform may be required to hold a capital markets services licence for ‘dealing in capital markets products (securities)’ under the SFA. In facilitating the offer of shares to persons in Singapore, prospectus registration requirements under the SFA will be triggered. It is possible to rely on a specific prospectus registration exemption for such purposes but the invocation of a prospectus registration exemption may carry certain advertising restrictions (i.e., restrictions on marketing the specific share). Another example is an automated digital advisory or asset management company, whose business activities may be construed as providing financial advisory services under the FAA or undertaking fund management under the SFA. It is possible that the fintech company had proposed (in its licence application to an authority) to only deal with ‘sophisticated investors’ (i.e., accredited investors and institutional investors as such terms are defined under the SFA). Consequently, the relevant licence granted to the fintech company may have a condition that restricts its dealings to ‘sophisticated’ investors when carrying out automated digital advisory or asset management activities. Such a condition would restrict the ability of the fintech company to market its services to retail investors.
Cross-border issues

There is no concept of ‘passporting’ of a fintech product or service under Singapore law. The fact that a fintech company is licensed in a foreign jurisdiction does not allow it to undertake regulated activities in Singapore simply on the basis that it is licensed in the foreign jurisdiction. Regardless of its licensing status in another jurisdiction, the offering of fintech products and services to persons in Singapore may trigger licensing requirements in Singapore on the part of the offeror, which depend on the actual type and scope of the products and services being offered.

What happens if a fintech company does not specifically target persons in Singapore in respect of its fintech product or service? The licensing requirements under the FAA and the SFA may still be triggered as they have extraterritorial effect. The relevant legislation provides that ‘where a person does an act partly in and partly outside Singapore which, if done wholly in Singapore, would constitute an offence under this Act, that person shall be guilty of that offence as if the act were carried out by that person in Singapore wholly in Singapore, and may be dealt with as if the offence were committed wholly in Singapore’. Furthermore, even where an act is done entirely outside of Singapore, licensing requirements would still apply if such conduct has a ‘substantial and reasonably foreseeable’ effect in Singapore. In this regard, there is no bright line test as to when conduct will be seen to have a ‘substantial and reasonably foreseeable’ effect in Singapore and such an analysis should be undertaken on a case-by-case basis. One factor (of many) that should be considered is that there has been no marketing of the fintech product or service to persons in Singapore.

III DIGITAL IDENTITY AND ONBOARDING

For access to electronic services provided by the Singapore government and its statutory boards, such as filing of income taxes and paying parking fines, the Government Technology Agency (GovTech) issues and manages a national digital identity for individuals known as the ‘SingPass’. Currently, Singapore citizens and permanent residents, as well as holders of certain documents that permit residency in Singapore (e.g., holders of employment passes and dependent passes), are eligible to register for a SingPass account.

SingPass also controls access to the MyInfo service, which is a store of their personal data either retrieved from Singapore government sources, or provided directly by that individual. While MyInfo was first designed for use by the Singapore government and its statutory boards, over 90 private-sector services including several financial service providers have now been permitted to use MyInfo to do away with the need for users to submit supporting documents when opening new bank accounts, applying for credit cards, purchasing life insurance or carrying out certain property transactions.

GovTech also issues and manages a corporate digital identity known as ‘CorpPass’. Both locally and foreign registered entities are eligible to register for a CorpPass account, which in 2019 became the only login method for corporate transactions with the Singapore government.

The national digital identity (NDI) system being developed by GovTech as part of the Singapore Smart Nation initiative will include a national facial recognition service, which will perform verification against the national biometric database over the internet. It is also reported that GovTech has been working with various private sector entities to test the NDI and further develop services that make use of the NDI. These services are expected to eventually include the signing of digital agreements and secure storage of digital documents.
It is potentially possible for financial service providers to carry out fully digitised onboarding of clients. However, they would need to consider (and accept) electronic risk such as the following:

a) integrity: the integrity of the electronic record (i.e., that the electronic record has not been altered or tampered with);

b) identity: the identity of the parties involved, including whether they are authorised to issue such electronic records; and

c) authority: where a client is a corporate entity, there is the additional risk of proving that the party issuing the electronic record or carrying out the electronic transaction has the requisite authority to transact on behalf of the client.

Depending on the particular type of financial services being provided, the provider would also need to consider relevant regulatory licensing issues.

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

The marketing and management of collective investment schemes, and the provision of equity crowdfunding platforms, peer-to-peer lending platforms and payment services, will typically fall within the scope of regulated activities in Singapore. Fintech companies that intend to offer such products and services should consider whether they will require a licence and whether licensing exemptions may be relied on (if so desired).

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

There is no specific regulation of blockchain technology on its own. However, the manner in which blockchain technology is used and the product or service that is offered (based on blockchain technology) may be construed as a regulated activity.

Depending on the characteristics of the digital token, digital tokens could be construed as a form of security such as a debenture or share, a unit in a collective investment scheme or even a derivatives contract. If the digital tokens issued in an initial coin offering fall within the definition of securities, a collective investment scheme or derivatives contracts under the SFA (or display characteristics similar to such capital markets products), it will raise potential financial regulatory issues under the SFA and other laws pertaining to financial regulation in Singapore. These include (among other things) prospectus registration requirements on the issuer for an offer of securities, units in a collective investment scheme or securities based derivatives to persons in Singapore and, possibly, licensing issues such as those for dealing in capital markets products by the issuer or intermediaries. In addition, platforms facilitating secondary trading of such digital tokens may also have to be approved or recognised by MAS as an approved exchange or recognised market operator respectively under the SFA.

In addition, digital tokens could be characterised as 'e-money' or 'digital payment tokens'. Depending on the nature of their usage or the services that are associated with them, such services could be construed as a payment service under the Payment Services Act. This could in turn mean that such payment services may need to be licensed under the Payment Services Act, unless a licensing exemption applies.

In general anti-money laundering and combating the financing of terrorism (AML and CFT) rules apply to financial institutions that deal in cryptocurrencies and tokens.
and financial institutions that have customers that deal in cryptocurrencies and tokens. The relevant notices and guidelines that are imposed on financial institutions provide that financial institutions will need to identify the AML and CFT risks in relation to new products and new business practices, including new delivery mechanisms and new or developing technologies that favour anonymity. Given that cryptocurrency transactions often involve anonymous transactions at some level, we would expect MAS to require financial institutions to pay particular attention to cryptocurrency-related transactions or transactions arising from cryptocurrency-related transactions.

VI OTHER NEW BUSINESS MODELS

There is no mandatory Singapore law that disqualifies self-executing contracts or ‘smart contracts’ (i.e., those that automatically self-execute if certain conditions are met), from being valid and enforceable under Singapore law.

There is no special legal framework that applies specifically to such contracts. These contracts would, of course, need to be valid under general law (e.g., the contract must fulfill the key elements for the formation of contract under Singapore law, including; offer and acceptance; consideration; and intention to create legal relations).

It is possible to enter into contracts electronically under Singapore law. Subject to exceptions, the general rule under the Electronic Transactions Act (ETA) is that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record. The ETA also provides that in the context of the formation of contracts, an offer and the acceptance of an offer may be expressed by means of electronic communications. Where an electronic communication is used in the formation of a contract, that contract shall not be denied validity or enforceability solely on the ground that an electronic communication was used for that purpose. A correction mechanism such as arbitration and mediation can be made available – the dispute resolution method could be encoded into the contract.

A fully automated investment process (e.g., ‘robo-advice’) and third-party websites comparing products or providing information about financial products will typically fall within the scope of regulated activities in Singapore, although the precise scope of the investment process and the particular financial products being offered will affect the

---

2 Section 4(1) of the ETA, read together with the First Schedule to the ETA, provides that the entirety of Part II of the ETA does not apply to the following categories of documents: (1) the creation or execution of a will; (2) negotiable instruments, documents of title, bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money; (3) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts; (4) any contract for the sale or other disposition of immovable property, or any interest in such property; and (5) the conveyance of immovable property or the transfer of any interest in immovable property.

3 ‘Electronic record’ is defined very broadly as ‘a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another’. ‘Information’ includes ‘data, text, images, sound, codes, computer programs, software and databases’.

4 ‘Electronic communication’ is defined as ‘any communication that the parties make by means of electronic records’.

5 Section 11 of the ETA.
Fintech companies that intend to offer such products and services should consider whether they will require a licence and whether licensing exemptions may be relied on (if so desired). Both of these models will also be subject to intellectual property and data protection considerations, as further discussed in Section VII below.

Some fintech products and services that are relatively new in Singapore include various products built in reliance on blockchain, products that purport to have deep or self-learning or AI aspects, and alternative authentication methods (replacing hardware security tokens). The regulatory and legal issues that they raise are dependent on the precise scope of the product or service being offered as well as the method through which the product is made available to the market. As an example, some products are developed for provision to ‘traditional’ financial institutions, where that financial institution maintains the client relationship. With this model, different MAS requirements may be relevant – for example, the fintech company may wish to engage the financial institution on the basis that its solution is compliant with Guidelines on Outsourcing Risk Management.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Fintech business models and related software may be protected by various intellectual property rights in Singapore. Patent protection may be available, and IPOS recently launched a new FinTech Fast Track initiative that facilitates a faster patent application-to-grant process for fintech inventions. Alternatives to patent protection include copyright or protection as trade secrets or confidential information, depending on the nature of the business model. Software would generally be protected by copyright. It is not necessary to carry out any registration in Singapore to obtain copyright protection.

If an employee develops an original work in pursuance of the terms of his or her employment, the default rule is that ownership of the copyright in the original work vests in the employer. If a contractor develops an original work, the default rule is that the contractor continues to own the original work. However, it is common for employees and contractors to be bound by written contractual obligations that specify ownership of the intellectual property they develop, and these default rules may be overridden. Fintech companies should ensure that their employees and contractors enter into such agreements.

The Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA) would apply to client data to the extent that it comprises personal data, which is defined as ‘data, whether true or not, about an individual who can be identified (a) from that data, or (b) from that data and other information to which the organisation has or is likely to have access’. In brief, there are two key parts of the PDPA:

- protection of an individual’s personal data, including in relation to requiring consent, granting access and correction rights, requiring reasonable security, and limiting transfers overseas; and
- establishment of a do-not-call registry for individuals to opt out from receiving certain types of marketing messages addressed via Singapore telephone numbers.

Internet protocol solutions may still be subject to the do-not-call registry (e.g., one such solution subject to this regime is WhatsApp).

Client data will also be protected by the common-law obligations of confidentiality. A recipient of data would be subject to confidentiality restraints where data or information in question is:
confidential as regards the giver of the data or information; and
imparted under circumstances where the recipient knew or ought to know that the data or information in question was confidential.

If confidential information is disclosed without consent, there is a risk that such disclosure would be in breach of confidence.

Singapore also has sector-specific regimes to protect the privacy and confidentiality of bank customer information and the confidentiality of information relating to trusts, including information of settlors and beneficiaries of trusts. While there are no special rules specifically focused on regulating the digital profiling of clients, it would be relevant to consider the PDPA and the various other data protection and privacy-related regimes in the implementation of a profiling solution, especially for companies providing financial services.

VIII YEAR IN REVIEW

The current legal framework governing payment services in Singapore is found in different pieces of legislation and certain parts of such legislation may not be easily applicable to an online context. In 2016, MAS embarked on a review of the regulatory framework governing payment services in Singapore with a view to modernising and streamlining the existing frameworks to encourage the wider adoption of electronic payments (e-payments) in Singapore. Arising from this review, MAS consulted twice on the proposed activity-based Payment Services Bill (the Bill) in August 2016 and November 2017. MAS also consulted on a set of guidelines to standardise and enhance the protection given to users in the context of unauthorised or mistaken payment transactions. On 14 January 2019, the Bill was passed in Parliament. The Payment Services Act came into effect on 28 January 2020 and, perhaps in line with this act, there appears to have been an increase in the number of e-payment companies entering the Singapore market.

IX OUTLOOK AND CONCLUSIONS

When we first started advising on fintech-related matters, many of the fintech companies were not looking to be licensed and wanted to structure their product or service such that they may rely on available licensing exemptions. Subsequently, as certain models of fintech products and services became more common (e.g., peer-to-peer lending and equity crowdfunding models), MAS provided greater guidance on the regulatory treatment of these models. Following on from this, there was a shift towards fintech companies seeking to be licensed. We believe that the current models of fintech companies will probably persist but the manner in which they will be operationalised will change. In this respect, we believe that many of these models will utilise blockchain technology in their products or services. It is also likely that other models leveraging blockchain technology will appear in the market (e.g., tokenised assets).
I OVERVIEW

Currently, there are no prohibitions or restrictions for certain types of fintech businesses in South Korea, nor is there an existing regulatory regime that specifically regulates cryptocurrency or blockchain. However, fintech businesses are likely to be subject to existing Korean laws and regulations, depending on the specific nature of the business undertaken. For example, certain financial activities of fintech companies may be regulated under existing Korean financial laws such as the Electronic Financial Transaction Act (EFTA).

As to the Korean government’s stance, financial regulators and policymakers are generally receptive to fintech innovations and technology driven new entrants to regulated financial services markets in South Korea. The Korean government has identified fintech as one of its 24 key areas to support innovation as a means to spur growth in the Korean financial industry. For example, the Korean government established the Fintech Support Centre that provides guidance on fintech-related projects and an opportunity for fintech start-ups to present their services to financial institutions. The Financial Services Commission (FSC) has announced 24 key projects for ‘financial innovation’ to be implemented as part of their 2020 business plan, and support for the fintech industry is one of the FSC’s key initiatives.

In terms of specific fintech-friendly policies, the Special Act on Support of Innovation of Finance (the Special Act) became effective on 1 April 2019 and introduced the regulatory sandbox scheme in South Korea. The new law introduced expedited confirmation on regulation and relaxed regulatory standards for those financial services designated as ‘innovative financial service’ by the government. In 2019, a total of 77 companies were designated as providing innovative financial services and accepted in the regulatory sandbox.

Furthermore, the Korean government offers special incentive schemes mainly in the form of tax incentives for tech and fintech businesses or small- and medium-sized (SME) businesses in South Korea. Notably, SME businesses established in certain areas of South Korea that are not highly populated cities can receive 50 per cent corporate tax relief for up to five years on their business income. Also, those companies identified as a ‘venture business’ by the Korean government, by which many fintech companies may qualify, may receive 50 per cent corporate tax relief even if they are located in highly populated cities in South Korea. For certain R&D costs (including labour costs and material costs), R&D tax deduction may be available as well.

---

1 Jung Min Lee and Joon Young Kim are senior attorneys and Samuel Yim is a senior foreign attorney at Kim & Chang.
Despite promoting policies conducive to fintech businesses, however, the Korean government has also shown concern for anti-money laundering (AML) and other consumer protection matters. The FSC amended the Anti-Money Laundering Guidelines for Cryptocurrencies (AMLC Guidelines) in 27 June 2018, requiring, among other things, that financial institutions enhance monitoring for accounts of cryptocurrency companies used for operating expenses and share the list of foreign cryptocurrency companies.

The Policy Committee of the National Assembly passed the proposed amendment to the Act on Reporting and Using Specified Financial Transaction Information (Proposed Amendment) that will subject virtual asset service providers (VASP) to AML requirements. The Proposed Amendment is significant in that it would bring the domestic cryptocurrency market, which has not been directly regulated, into the regulatory framework in South Korea.

II REGULATION

i Licensing and marketing

Currently, there are no prohibitions or restrictions for certain types of fintech businesses in South Korea. However, fintech businesses providing certain financial services are required to obtain a licence under the relevant Korean financial laws and regulations.

Specifically, the EFTA is the law that regulates electronic financial transactions in South Korea. The EFTA covers the:

- rights and obligations of the parties to an electronic financial transaction;
- provisions to ensure the safety of electronic financial transactions and protection of users; and
- authorisation, registration and specific scope of activities of electronic financial businesses.

Activities listed as 'electronic financial business' under the EFTA include the:

- issuance and management of electronic currency;
- electronic funds transfer services;
- issuance and management of electronic debit payment services;
- issuance and management of electronic prepayment services;
- electronic payment settlement agency services;
- depository service for settlement of transactions; and
- intermediary electronic collection and payment services between payors and payees.

Other than the issuance and management of electronic currency, which needs to be licensed by the FSC, the above types of electronic financial businesses must be registered with the FSC and are supervised by the FSC and the Financial Supervisory Service (FSS).

Further, fintech businesses that do not engage in electronic financial business activities under the EFTA but intend to undertake regulated activities in South Korea, such as banking or credit card businesses, should review whether it is required to obtain appropriate authorisation (licence or registration) from the relevant Korean regulatory authorities such as the FSC or the FSS.

ii Regulatory sandbox

The Special Act, enacted in 31 December 2018 and effective on 1 April 2019, introduced the regulatory sandbox scheme in South Korea. The Special Act introduces the following:
Expedited confirmation on regulation
Under this scheme, a financial company that plans to start a new type of financial business may deem that no regulation on the new business exists if the company does not receive a response from the FSC within 30 days after filing an inquiry to the FSC as to the existence of a regulation on the new business. The FSC may forward the inquiry to other relevant government agencies if they think necessary, but in any case they must provide a response within 30 days.

Designation of innovative financial service
A financial service that is designated ‘innovative’ by the government may operate free of regulation and without legal grounds for operation for a designated period (this period lasts for up to two years and may be renewed once for up to two years). Financial service providers who believe that their service is clearly distinguishable from pre-existing service in terms of content and methods may ask the government to designate it as an innovative financial service. Upon receiving an application, the Innovative Financial Services Examination Committee, which consists of public officials from the FSC and other relevant government agencies and private experts, will assess various factors, such as whether: the proposed innovative financial services are provided in South Korea; the proposed financial services is truly innovative; and the proposed financial service will likely further the customers’ interests.

In addition, if a designated innovative financial service is being operated under a licence required by other financial laws and regulations, the service shall be allowed an exclusive right of operation for two years after designation as an innovative financial service. This means that during the two-year period, no other service provider may provide the same type of financial service.

Cross-border issues
Where a fintech business established out of South Korea wishes to access new customers in South Korea, it will need to consider whether it requires authorisation from a Korean regulatory authority. A fintech business established outside of South Korea may be subject to Korean laws and regulations if it carries out regulated activities in South Korea. Where an overseas fintech business performs regulated activities in South Korea, it will need to obtain authorisation from the relevant Korean financial regulatory authority, as discussed in Section II(i) above. Generally, the standard, among others, to determine the applicability of Korean laws to foreign fintech businesses is whether the foreign fintech businesses targeted Korean customers (e.g., Korean website) or allowed payment in Korean won.

Regarding foreign exchange, the Foreign Exchange Transaction Act regulates foreign exchange businesses including the issuance or dealing of foreign exchange and payment, and collection and receipt thereof between South Korea and a foreign country. The Foreign Exchange Transaction Rule (FX Rule) is a subordinate regulation of the Foreign Exchange Transaction Act. The FX Rule was recently amended and became effective on 8 October 2019. The amended FX Rule increased the annual limit for overseas remittance by institutions registered as small-amount remittance operators from US$30,000 to US$50,000 per customer. Also, from 8 October 2019, securities companies and credit card companies may remit funds overseas as long as the amount does not exceed US$5,000 per remittance and US$50,000 per year. In addition, electronic currencies and prepaid electronic payment means issued in South Korea may now be used in foreign jurisdictions to pay for goods or services or be exchanged to foreign currencies.
III DIGITAL IDENTITY AND ONBOARDING

There is no digital identity that is generally recognised in South Korea. However, a certificate of authentication used for the purpose of self-authentication does exist. Certificates of authentication can be issued by an authentication certification institution designated by the government (such as the Korea Financial Telecommunications and Clearing Institute), and such certificates of authentication are typically used for when self-authenticating online. Under the Real Name Financial Transaction Law, verification of real name is necessary in order to conduct financial transactions. Therefore, in principle, financial institutions must onboard by undertaking customer verification procedures offline through a face-to-face method. However, there are exceptions where undertaking customer verification procedures through a non-face-to-face method is permitted. Where customer verification procedures are undertaken through a non-face-to-face method, two of the methods from among (a) to (d) below need to be selected, and it is recommended that the financial company select on its own an additional verification method (either (e) or (f)).

(a) present a copy of identification card (e.g., submit online a photo or scanned copy of one’s identification card);
(b) video call (e.g., an employee of the financial company compares the picture on the identification card with the customer’s face);
(c) verify upon receiving delivery of credit card (e.g., an employee of the delivery company verifies real name through a voucher);
(d) use of existing account (e.g., verify the customer’s transaction authority for a given account through transfer of small amounts, etc., from an account opened at another financial company);
(e) use of the verification results of another institution (e.g., verify identity at another institution such as a certification institution, and then use the issued certification of authentication, IPIN, mobile phone number, etc.); and
(f) verify through other sources of personal information (e.g., compare personal information provided by the customer with information possessed by a credit information agency).

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

Under Korean laws, businesses related to financial investment products such as collective investment businesses are fundamentally regulated by the Financial Investment Services and Capital Markets Act (FSCMA), with regulations differing for each specific type of business.

i Crowdfunding

The FSCMA regulates securities-type crowdfunding, and in order to conduct securities-type crowdfunding, registration needs to be made as an ‘online small-sized investment broker’ with the FSC in accordance with the FSCMA.

Crowdfunding was introduced in 2016 for the financing of start-ups and venture businesses. There are, however, certain restrictions in the issuance of equity for crowdfunding under the FSCMA. Namely, a single company can raise funds up to 1.5 billion Korean won per year through crowdfunding. To raise funds that exceed 1.5 Korean billion won, conventional means of financing should be utilised. Moreover, under the FSCMA, the issuance of equity for crowdfunding is permitted for non-listed SMEs with less than seven years of business operations.

© 2020 Law Business Research Ltd
In 10 April 2018, the Enforcement Decree of the FSCMA was amended to increase the limit for an ordinary investor to invest in crowdfunding from 5 million Korean won to 10 million Korean won per year with an issuer of equity. In addition, the amended Enforcement Decree of the FSCMA allowed social enterprises, which are companies certified by the Ministry of Employment and Labour that seek to improve financial, social and environmental well-being through commercial activities (e.g., providing employment opportunities to disadvantaged groups or making contributions to the local society) to raise funds through crowdfunding.

ii Crowd-lending and P2P lending
The Act on Online-linked Financing (P2P Act), which was enacted on 26 November 2019 to govern P2P lending, will become effective on 27 August 2020. The Presidential Decree of the P2P Act was published on 28 January 2020 and will be open for public comment until 9 March 2020. The major provisions of the P2P Act and the Presidential Decree are described below:

a a person who intends to provide P2P lending service shall have at least 500 million Korean won of equity capital, adequate human resources and physical facilities, and register with the FSC;
b P2P lending businesses shall charge fees only at rates announced on their online platforms;
c principal investing by P2P lending service providers permitted only when more than 80 per cent of investments for P2P loan balance have been raised;
d P2P lending to the same borrower will be limited to 7 per cent of the P2P loan balance or 7 billion Korean won. For P2P lending operators whose loan balance is below 30 billion Korean won, the lending cap to the same borrower will be set at 210 million Korean won;
e individual investors may lend up to 5 million Korean won to the same borrower for a total of 50 million Korean won per year. Accredited investors may lend up to 20 million Korean won to the same borrower for up to 100 million Korean won per year; and
f a central registry will be set up to manage and maintain up-to-date information about online P2P financing transactions, such as information about borrowers and investors, and will also manage limits on loans and investments.

iii Loans or financings on a secondary market
In the case of securities acquired through crowdfunding, it is obligatory to deposit at a securities depository or make a safety deposit, and for a period of six months, transfer cannot be made other than to professional investors and persons specified under the FSCMA.

For rights to acquire principal and interest obtained through P2P lending, in principle, transfer is possible depending on the method of bond transfer. However, there are cases where a P2P lending business restricts transfer through its terms and conditions.

If a right that is acquired through investment is deemed a security under the FSCMA owing to the possibility of transfer, risk of loss of principal, etc., the issuer of such bond and the broker business must obtain financial investment business licences in accordance with the FSMCA and will be strictly regulated with regards to issuance and distribution of securities. Therefore, caution needs to be exercised to prevent being deemed a security.
Payment licence

In order to run a payment service, registration needs to be made as a payment gateway (PG) with the FSC.

Upon registering as a PG, obligations under the EFTA are applied, and the PG is subject to supervision and inspection by the FSS.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

There is no existing regulatory regime or statute that specifically regulates cryptocurrency or blockchain businesses in South Korea. However, the Korean regulators are likely to apply or enforce existing Korean laws and regulations for cryptocurrencies.

For example, in an initial coin offering (ICO), if tokens are classified as ‘securities’ under Korean law, the tokens will then be subject to the offering restrictions in South Korea under the FSCMA. Or, even if tokens are not classified as securities, if the marketing of the tokens in an ICO raises funds from the public with a promise to return the original investment amount, or an amount exceeding such investment in the future, the ICO could be regulated by the Act on the Regulation of Conducting Fundraising Business without Permission.

The Korean government has taken steps towards introducing potential cryptocurrency and ICO regulations, of which key developments are discussed below.

i Cryptocurrencies

In 2017, South Korea experienced a dramatic increase in the volume of cryptocurrency trading where the trading volume for a 24-hour period in the Korean cryptocurrency exchanges averaged up to 8 trillion Korean won.

In response to this high volume of cryptocurrency trading, in September 2017, the Korean government formed an intergovernmental task force to create and implement cryptocurrency regulations. The government agencies that participated in this task force were the Ministry of Strategy and Finance, the Ministry of Justice, the FSC and other relevant regulatory authorities. In the ‘Government Announcement on Cryptocurrency’ released in December 2017, the Korean government announced that it will take measures to curb the recent speculation in the cryptocurrency market.

As a part of such measures, on January 30, 2018, the Korean Financial Intelligence Unit (FIU) announced the AMLC Guidelines, enforceable for financial institutions that transact with cryptocurrency companies. Notable requirements of the AMLC Guidelines are as follows:

a real-name verification is required for payment and receipt to cryptocurrency companies-

• users are only allowed to make payment to and receive payment from a cryptocurrency company’s bank account using their own real-name verified account that has been opened under the same bank as the cryptocurrency company; and
• financial institutions may decline transactions with cryptocurrency companies that make payments to or receive payments from its users that do not use real-name verified bank accounts;

b customer due diligence -
financial institutions must put in place a process to check whether a customer is a cryptocurrency company; and

financial institutions must verify, through on-site due diligence, certain additional information pertaining to cryptocurrency companies (including whether the cryptocurrency company is maintaining separate transaction records for each customer) at least every six months; and


c) suspicious activity reports -

financial institutions must appoint dedicated staff for monitoring suspicious transactions of cryptocurrency companies and their users; and

financial institutions must establish stronger transaction monitoring rules for suspicious activities of cryptocurrency companies.

In April 2018, the FSC conducted a monitoring of compliance with the AMLC Guidelines. Based on the monitoring, the FSC amended the AMLC Guidelines on 27 June 2018. The latter became effective on 10 July 2018 and will remain effective until July 2020. The key requirements of the amended AMLC Guidelines are as follows:

a) financial institutions shall enhance monitoring for accounts of cryptocurrency companies that are used for operating expenses, and conduct enhanced customer due diligence if it identifies a suspicious transaction;

b) financial institutions shall share the list of foreign cryptocurrency companies; and

c) if a financial institution refuses to transact with a certain cryptocurrency company, the financial institution shall specify the timing and grounds for its refusal.

The Policy Committee of the National Assembly passed the proposed amendment on 25 November 2019. Thereafter, the Legislation and Judiciary Committee would review the proposed amendment and then send it to the plenary session of the National Assembly for resolution. However, as of the date of this analysis, it is not clear whether the proposed amendment will pass the plenary session before the General Election of the National Assembly on 15 April 2020, when members of the National Assembly are newly elected. If the proposed amendment does not so pass the plenary session by then, the proposed amendment will need to go through the legislative procedures of the National Assembly de novo. The key provisions in the proposed amendment are set out below.

**Reporting requirements for VASPs**

VASPs professionally engaged in the (1) sale and purchase of virtual assets, (2) exchange of virtual assets, (3) mediation or arrangement of (1) and (2), and (4) storage or management of virtual assets must report the company name, the representative’s name, the location of

---

2 The National Assembly is the legislative body of South Korea, which is equivalent to the US Congress.

3 South Korea is a member state in the Financial Action Task Force (FATF), a global multinational organisation that was created to establish international standards for AML and combating the financing of terrorism (CFT) and require other member states to comply with such standards. Following a plenary meeting held in February 2018 where the FATF discussed the risk of money laundering and financing of terrorism using virtual assets and countermeasures, in October 2018, the FATF resolved to include AML and CFT requirements for VASPs in the FATF Recommendation. The FATF published the Interpretive Note with details in June 2019 and plans to monitor the implementation status of Member States at around June 2020. In order to comply with the FATF Recommendation, the Korean legislature has drafted the proposed amendment for resolution by the National Assembly.
the business place, and contact information to the Commissioner of the FIU in advance and have the report accepted by the FIU. Failure to report will result in criminal punishment by imprisonment of up to five years or a fine of up to 50 million Korean won.

**AML requirements for VASPs**

As with other financial institutions, VASPs will be subject to various AML requirements, including suspicious transaction report (STR), currency transaction report (CTR), and customer due diligence (CDD), and will be required to set up an internal control system to fulfil such requirements in good faith and to separately manage transaction details by customer.

**Expanded CDD on financial companies**

In addition to the existing CDD items, a financial company must ensure that a VASP has satisfied requirements for acceptance of report and the requirement to separately manage deposits from customers and its own property, among others. Furthermore, a financial company must refuse or terminate transactions with the VASP if it does not have a valid report, an ISMS (information security management system) certification, a real name deposit and withdrawal account, or is otherwise unqualified.

**Initial coin offerings**

In September 2017, the FSC issued a press release prohibiting ICOs in South Korea, but no laws or regulations have yet to been enacted to enforce this prohibition of ICOs. Subsequently, on 31 January 2019, the Korean government announced the result of its monitoring of the ICO practice in South Korea and its proposed approach in regulating ICOs. In this announcement, the Korean government stated that they identified companies bypassing the government’s prohibition on ICOs by performing ICOs through paper companies in foreign jurisdictions (such as Singapore) while raising funds from domestic investors. The Korean government announced that such practice substantively constitutes domestic ICOs albeit in the form of a foreign ICO. Moreover, the Korean government stated that domestic investors were at significant risk due to such practice because the companies performing the ICOs did not disclose substantial information for the investors to make an informed decision.

In addition, the Korean government also deemed that certain ICO projects may violate the FSCMA if an ICO project involves issuance and transaction of P2P collateralised loan tokens; sale of cryptocurrencies investment funds; or operation of unauthorised financial investment business by providing investment services with ICO tokens.

Considering that ICO poses high investment risks and lacks a global regulatory framework, the Korean government announced that it will take a conservative approach in legalising ICOs. In the same vein, the Korean government maintained an equivocal position as to whether it will publish an ICO guideline, saying that the government's issuance of such guideline may give the market a wrong impression that the government officially approved domestic ICOs.
VI OTHER NEW BUSINESS MODELS

i Robo-adviser

‘Robo-adviser’, is a derivation of the words robot and adviser, is an automated online asset management service that uses IT technologies such as AI to provide appropriate personalised portfolios for investors. It provides services at substantially lower fees than that of existing asset management services, and future development is anticipated in terms of convenience and low cost. Financial institutions in South Korea have, in some respects, either implemented robo-advisers or are preparing to do so.

Depending on the type of service provided, registration needs to be made as an investment advisory business or a discretionary investment management service in accordance with the FSCMA.

To promote the robo-adviser industry, the FSC recently announced a proposed amendment relating to robo-advisers that would:

a lower the shareholders’ equity needed for non-face-to-face discretionary investment management services that utilise robo-advisers from 4 billion Korean won to 1.5 billion Korean won in order to facilitate the entry of fintech businesses other than existing financial institutions into the robo-advisory industry;

b allow robo-advisers to manage fund assets; and

c allow not only asset managers but also robo-advisers to be consigned with and manage funds and discretionary assets.

ii My Data Businesses

The amendment of the Use and Protection of Credit Information Act (the Credit Information Act) was followed by the introduction of ‘Personal Credit Information Management Businesses’ (My Data Businesses), which provide information principals with services such as comprehensive inquiry of their own data, recommendation of optimal financial products, and advice on financial products. My Data Businesses are businesses that provide professional support for the individual who is the information principal to efficiently manage and use his or her own information.

My Data Businesses integrate and search one’s credit information, analyse financial statuses, and provide personalised financial consulting. Furthermore, My Data Businesses can provide services that present a list of accessible financial products for each individual consumer given, among others, his or her credit situation or financial status, and compare in detail prices and benefits of each product to recommend financial products optimised for each individual.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

i Intellectual property

In South Korea, innovations and inventions can be protected by IP rights such as patents, utility models, designs, copyrights and trade secrets. Korean law explicitly provides for the protection of patents under the Patent Act, utility models under the Utility Model Act, designs under the Design Protection Act, copyrights including copyrights in computer software under the Copyright Act and trade secrets under the Unfair Competition Prevention Act (UCPA).
Under current Korean Intellectual Property Office (KIPO) practice, fintech inventions relating to software or business methods that include only abstract ideas or mental steps do not qualify as inventions. However, under KIPO’s ‘Examination Guidelines for Computer-related Inventions’, business methods can be patented if the inventions are properly claimed so as to define physical means to achieve a specific purpose that has practical application in the industry. Further, although software per se is not patentable at this time, computer-readable media for implementing software is patentable subject matter.

Graphical user interfaces of fintech software may be protected by design registrations under the Design Protection Act. For example, images represented on a display portion of a product such as a display panel can be registered and protected as a design. Copyright protection is also possible upon creation of an original computer program without formal registration requirements. Although a copyright registration is not a prerequisite for copyright protection or enforcement, it provides certain advantageous statutory presumptions in enforcing the copyright. The source code of fintech software may be protected as a trade secret under the UCIPA. The UCIPA defines a trade secret to mean information of a technical or managerial nature that is useful for business activities, is generally unknown to the public, possesses independent economic value and is maintained as a secret.

Ownership of IP rights such as patents, utility models, and designs initially belong to the person who created such rights. Such person may transfer his or her IP ownership right to another party through an agreement. However, transfer of an IP right, other than through inheritance or other general succession, is not effective in South Korea against third parties unless it is recorded at KIPO.

In the context of an employer-employee relationship, there are two ways for the employer to obtain ownership rights to in-service inventions of its employees. First, the employer may enter into a pre-invention assignment agreement with an employee with a provision that the employee agrees to assign any and all future in-service inventions to the employer. Second, the employer may adopt an employment rule such as an invention remuneration policy that expressly provides for employee-inventors to assign any and all future in-service inventions to the employer and the employer to provide remuneration to such employee-inventors. In either case, if the employer chooses to acquire the ownership right to an in-service invention pursuant to the agreement or employment rule, the employee is entitled to ‘reasonable compensation’ from the employer.

Ownership of copyright initially belongs to the actual author or authors of a given work. In the context of an employer-employee or work-for-hire relationship, however, an employing legal entity, organisation, or person may be deemed to be the author of a work with ownership of copyright in the work. Under the Copyright Act, such employer is deemed to have copyright ownership of a work if the work is created by an employee within the scope of employment and made public (computer programs do not need to be made public), subject to the employer’s supervision, and there is no separate or particular contract or employment regulation providing that the status of the author of, or ownership of copyright in, the work-for-hire should belong to the employee.

For IP rights such as patents, utility models, and designs, the party enforcing an IP right should own the registered rights in South Korea. For copyrights, works by foreigners, such as the source code of fintech software, are entitled to protection under treaties to which South Korea has acceded. However, the Copyright Act provides exceptions to favourable treatment of foreigners’ copyrights under such treaties. In particular, the Copyright Act provides that even if the copyright protection period for foreigners’ copyrights may be in

© 2020 Law Business Research Ltd
force and entitled to protection under the Copyright Act, if the copyright protection period granted in the country of their origin has already expired, South Korea will not recognise the copyright protection period.

IP rights including patents, utility models, and designs are a type of property right and thus, owners of IP rights may exploit or monetise them for their benefit. For example, an IP owner may assign or sell his or her IP right to another person or entity and receive payment in return. An IP right may also be pledged as collateral for a loan or investment from another person or entity. Further, an IP right may be licensed through an exclusive or non-exclusive agreement for royalties or may be licensed to another party in a cross-licence agreement. If an IP right is jointly owned, a joint owner may license the IP right only with the consent of all the other joint owners, but each owner may still freely practise the jointly owned IP.

IP-related licences may be subject to governmental review under certain circumstances. For example, under the Fair Trade Law, the Fair Trade Commission has released the Guidelines on the Unfair Exercise of IP Rights (the IP Guidelines), for examining licence agreements. If a provision of a licence agreement violates one of the standards set forth in the IP Guidelines, a court may find such provision to be null and void as being contrary to Korean public policy.

ii Personal data

In South Korea, the protection and regulation of personal data is primarily governed by the Personal Information Protection Act (PIPA). The PIPA is the overarching personal data protection law in South Korea that may apply to fintech businesses operating in South Korea. The PIPA prescribes detailed measures for each of the stages involved in the processing of personal data such as collection and use, provision to a third party, outsourcing and destruction. The PIPA must be followed by all personal information processing entities, which are defined as all persons, organisations, corporations and governmental agencies that process personal data for business purposes. Under the PIPA, data subjects must be informed of, and provide their consent to the following matters before their personal data is collected or used:

\[ a \] the purpose of the collection and use;
\[ b \] the items of personal information that will be collected;
\[ c \] the duration of the possession and use of the personal information; and
\[ d \] disclosure that the data subject has a right to refuse to give consent and the negative consequences or disadvantages that may result from such refusal.

In addition, the Credit Information Act complements the PIPA. The Credit Information Act regulates and protects financial transaction information and credit information of individuals and entities.

On 9 January 2020, the National Assembly passed the amendments to South Korea’s three main data privacy laws (Amendments): PIPA, the Act on the Promotion of the Use of the Information Network and Information Protection (Network Act), and the Credit Information Act.

The Amendments (1) clearly distinguish between personal data, pseudonymised data and anonymised data, and enact detailed provisions on the processing of pseudonymised data, (2) transform the Personal Information Protection Commission (PIPC) into the central data privacy regulatory authority, (3) transfer to the PIPA all privacy provisions in the previous Network Act relating to online service providers, and (4) clarify that the Credit Information Act, which used to apply mostly to the financial institutions, now also applies...
to all commercial companies and grant the PIPC the authority to request information, to investigate, to conduct on-site investigations, and to impose corrective orders and administrative fines for the purpose of enforcing the Credit Information Act. The effective date for the Amendments is 5 August 2020.

The Ministry of the Interior and Safety, the Korean Communications Commission and the Ministry of Science and ICT, and the FSC and the FSS used to be the responsible regulatory agencies for enforcing the PIPA, the Network Act and the Credit Information Act, respectively. With the Amendments passed on 9 January 2020, all enforcement of privacy regulations will be centralised through the PIPC. In addition, once a violation of a relevant privacy law is confirmed, the PIPC can impose administrative penalties, such as corrective orders and fines, and, as necessary, refer the case for criminal prosecution. Criminal sanctions can be imposed following an investigation by the police or prosecutor’s office, either on its own initiative or upon a referral by the relevant regulatory authority.

As for the applicability of these laws to overseas entities, the PIPA applies to all personal information processing entities regardless of whether they are located overseas, and the Credit Information Act would also apply to overseas entities handling financial transaction information and credit information of individuals or entities in South Korea. Although the PIPA and the Credit Information Act do not specifically address their jurisdictional scope for overseas entities, the Korean regulatory authorities have promoted to or ensured compliance by overseas entities with these privacy laws.

iii Cybersecurity

The main statute in the context of cybersecurity that applies to fintech businesses is the PIPA. It prescribes detailed technical security and administrative requirements for cybersecurity such as:

a. the establishment and implementation of an internal management plan for the secure processing of personal information;
b. installation and operation of an access restriction system for preventing illegal access to and leakage of personal information; and
c. the application of encryption technology to enable secure storage and transfer of personal information.

Further, the EFTA criminalises certain types of cyber activities that may apply to fintech businesses operating in South Korea. The EFTA criminalises cyber activities that:

a. intrude on electronic financial infrastructures without proper access rights or by surpassing the scope of permitted access rights or altering, destroying, concealing or leaking data that is saved in such infrastructures; and
b. destroy data, or deploy a computer virus, logic bomb or programme such as an email bomb for the purpose of disrupting the safe operation of electronic financial infrastructures.

iv Open banking system

The FSC launched a pilot programme for the ‘Open Banking System’ in the banking sector on 30 October 2019, which expanded to fintech firms on 18 December 2019. The open banking system enables bank customers to choose any mobile banking application to manage
all their accounts in a single application without having to use separate applications for different banks. The FSC stated that the government, to provide a legal basis, will revise the EFTA to expand the service scope and function of the open banking system.

Based on the FSC's roadmap, the transition to open banking system will be in three phases:

\( a \) Phase 1 will rely on banks’ voluntary agreement to an open banking system that would enable customers to use a single application to access their accounts at different banks.

\( b \) Phase 2 will require an amendment to be made to the EFTA to include the open banking system. The FSC is aiming to amend the EFTA by the second half of 2020.

\( c \) Phase 3 will establish the regime in which fintech firms gain direct access to the financial payment system. To be eligible for such direct access, fintech payment service providers will have to meet certain requirements of financial soundness and digital capabilities.

VIII YEAR IN REVIEW

Over the past three years, notable amendments were made to financial laws that may impact fintech businesses operating in South Korea. The landmark legislation was the amendments to the three main privacy laws of South Korea: the PIPA, the Network Act and the Credit Information Act. Among the areas of change, the amendments introduced the concept of pseudonymised data and allowed the use of pseudonymised data without the consent of individuals. In addition, in April 2018, the Enforcement Decree of the FSCMA was amended to increase the limit for ordinary investors’ investment in crowdfunding by 100,000 Korean won. As a result, an ordinary investor may now invest 5 million Korean won per year for an issuer of equity. Also, the amended FX Rule became effective on 8 October 2019 that increased the annual limit for overseas remittance by institutions registered as small-amount remittance operators from US$30,000 to US$50,000. Further, securities companies and credit card companies may remit funds overseas as long as the amount does not exceed US$5,000 per remittance and US$50,000 per year. In addition, electronic currencies and prepaid electronic payment means issued in South Korea may now be used in foreign jurisdictions to pay for goods or services or be exchanged to foreign currencies.

The P2P Act will govern P2P lending services in South Korea and become effective on 27 August 2020. Under the P2P Act, all P2P lenders are required to have equity capital worth at least 500 million Korean won and qualify as financial companies, and then file a registration with the FSC. In addition, the P2P Act permits financial companies and P2P lenders to invest in P2P lending not in excess of a certain percentage of P2P loans, and sets forth lending limits, investment limits and matters to be notified for protecting P2P investors and borrowers.

Furthermore, on 21 November 2019, a subcommittee of the National Assembly’s National Policy Committee passed a resolution on the Proposed Amendment. The Proposed Amendment is pending to pass the plenary session of the National Assembly. As for its position on ICOs, on 31 January 2019, the Korean government announced the result of its monitoring of the ICO practice in South Korea and its proposed approach in regulating ICOs. In this announcement, the government stated that they identified companies bypassing the prohibition on ICOs by performing ICOs through paper companies in foreign jurisdictions (such as Singapore) while raising funds from domestic investors. The government also deemed that certain ICO projects may violate the FSCMA. Considering that ICOs are high-risk investments and lack global regulatory framework, the Korean government announced
that it will take a conservative approach in legitimising ICOs. In the same vein, the Korean government maintained an equivocal position as to whether it will publish an ICO guideline, saying that the issuance of such guideline may give the market a wrong impression that the government has officially approved domestic ICOs.

Meanwhile, measures have been taken to promote fintech innovations in the financial services market in South Korea. The Special Act introduced the expedited confirmation on regulation and designation of innovative financial services.

Since the enactment of the Special Act, a total of 77 companies were designated as innovative financial services in 2019 and are currently operating in the regulatory sandbox.

IX OUTLOOK AND CONCLUSIONS

Recently, South Korea’s fintech environment has seen a variety of industries being established, and its related market is developing rapidly. Further, South Korea’s financial supervisory authorities have recently announced various policies to promote fintech. The fintech industry is anticipated to continue to grow quantitatively and qualitatively in 2020 as a result of various innovative financial services being accepted into the regulatory sandbox after the Special Act became effective on 1 April 2019.

Furthermore, there are two internet-only banks in South Korea, K-Bank and Kakao Bank, that received authorisation from the FSC and are currently in operation. In December 2019, the FSC granted a pre-authorisation to TOSS Bank, a subsidiary of a major fintech company called TOSS (Viva Republica), to become the third internet-only bank in South Korea.

Separately, the government conceptually differentiates cryptocurrency from blockchain technology. The government recognises the innovative nature of blockchain technology and its potential impact on the Korean economy. Although it has shown hesitation in endorsing or institutionalising cryptocurrencies and has repeatedly warned investors about the potential dangers of investing in them, it has expressed interest in fostering, promoting and investing in blockchain technology as part of its strategic and economic plans. Furthermore, while the central government appears to be uneasy about cryptocurrencies, some local governments have shown interest in issuing their own cryptocurrencies.
I OVERVIEW

There is currently no specific regulatory framework in Spain or the European Union governing fintech. However, both the European and the Spanish supervisory authorities are conscious of the increasing importance of this sector and they are currently analysing it with a view to eventually regulating it.

There are various electronic sources providing information on fintech. For instance, the Spanish Fintech and Insurtech Association has its own website and the National Securities Market Commission (CNMV) has created a section on its website aimed at establishing an informal communication space with fintech. Besides this, the CNMV has created a Q&A on fintech for activities and services where fintech may be involved.

The main tax incentive schemes for investment in tech or fintech businesses generally applicable in Spain are: (1) the Spanish patent box regime and the research, development, and innovation tax credit potentially applicable to Spanish-resident companies engaged in tech and fintech activities (generally only in those cases in which the technology qualifies, e.g., as a patent or as advance registered software), and (2) the corporate income tax benefits for start-ups (e.g., a 15 per cent rate for the start-up’s first two fiscal years, instead of the statutory 25 per cent rate) and Spanish-resident venture-capital entities, along with (3) tax credits for ‘business angels’ in specific start-ups (under specific conditions) represent. Proper structuring is essential for investors in these companies to mitigate any Spanish tax leakage applicable to investments in tech and fintech companies.

In general terms, and until further regulations are passed, Spain should be considered as a relatively fintech-friendly jurisdiction. By way of example, in 2013 it was estimated that there were 50 fintech companies in Spain; this number increased to 392 as at December 2019. In 2019, the fintech industry grew by 16 per cent.

II REGULATION

i Licensing and marketing

As stated in Section I, there is no specific regulatory framework in Spain governing fintech. As a result, there is no specific fintech licence nor are there any specific marketing rules that are applicable to fintech. This is mainly due to the fact that fintech businesses in Spain provide a variety of financial services. In general, leaving aside third-party providers (TPPs)
regulated under Directive (EU) 2015/2366 of the European Parliament and of the Council, of 25 November, on payment services in the internal market (PSD2) and crowdfunding and crowd-lending platforms, which are subject to Law 5/2015 of 27 April on the promotion of business financing (Law 5/2015), fintech business focused only on developing IT solutions to support the provision of services by financial entities are not currently subject to any financial regulatory regime.

However, fintech that engages in financial activities such as deposit-taking, investment services (such as automated digital advice and the management of collective investments), payment services and insurance, is subject to the general regulatory regime that applies to any company operating in those sectors (including marketing rules) and, therefore, has to obtain authorisation from the relevant authorities depending on the service rendered. For banking services, the competent authority would be the Bank of Spain (BoS) or the European Central Bank. In the case of investment services the competent authority would be the CNMV and for services or products that relate to insurance, reinsurance and pension funds it would be the General Directorate of Insurance and Pension Funds (DGSFP).

As stated above, Law 5/2015 regulates crowdfunding and crowd-lending platforms and the provision of their services. The performance of these activities is subject to obtaining an authorisation which is granted by the CNMV (with the intervention of the BoS). Unlike other financial regulations in Spain, which are transpositions of European financial directives, Law 5/2015 is purely domestic. However, this will probably change, since in March 2018 the European Commission published a proposal for a regulation of the European Parliament and of the European Council on European crowdfunding service providers for business (the Proposal). Although the Proposal will not apply to crowdfunding services that are provided by natural or legal persons in accordance with national law (such as those provided under Law 5/2015), the Proposal establishes that a legal person that intends to provide crowdfunding services shall apply to the European Securities and Markets Authority (ESMA) for authorisation as a crowdfunding service provider. The Proposal is unique because it is the first time that one of the European Supervisory Authorities has been allowed to grant an authorisation for the provision of a financial service within the European Union.

Apart from the above, and after a year of no progress, on 28 February 2020, the Ministry of the Economy finally published the latest Draft Law for the Digital Transformation of the Financial System, which was approved by the government in February 2019 (the Draft Bill). The objectives of this law are: (1) ensuring that the financial supervisory authorities have adequate instruments to keep performing their supervisory and regulatory functions within the new digital environment; and (2) facilitating the innovative process in order to achieve better access to financing by productive sectors, more efficient financial services and a greater attraction of talent in a highly competitive international environment. In line with promoting digital innovation, the Draft Bill, once approved, will implement a regulatory sandbox in Spain, which intends to include both private and general interest projects. Following the commencement of the parliamentary process, it is predicted that the Draft Bill will be approved around mid-June 2020.

In this line of promotion of digital innovation, the Draft Bill implements a regulatory sandbox in Spain, the terms of which will be unknown until the final text of the Draft Bill is published. The Draft Bill is under discussion and there is no specific deadline for its passing.

Since there is no specific regulatory framework in Spain governing the marketing of fintech products and services (except for Law 5/2015), these entities must observe the marketing legislation applicable to any other company. Apart from the Spanish law on the
protection of consumers, which establishes certain principles on marketing, and the general law on publicity, other applicable publicity provisions are included within the Spanish laws on electronic commerce and distance marketing of financial services.

In Spain, there are negative credit information registries that may be accessed by any natural or legal person in accordance with certain rules. The BoS handles the Risk Information Centre (CIR), which contains information on loans, credits, bank endorsements and general risks regarding customers, provided by the reporting institutions (such as credit entities) and that may only be accessed by natural or legal persons who are holders of risks declared to the CIR in accordance with certain rules.

ii Cross-border issues

There are no particular passporting procedures available for fintech. Only fintech set out as regulated financial services providers would have access to the cross-border provisions under Spanish laws implementing the European directives that allow for specific types of regulated entities to operate in another country without having to be authorised by their local regulators.

Accordingly, EU-regulated financial services providers benefit from the passporting procedure, which enables them to provide services in Spain on a freedom-to-provide-services basis or by establishing a branch. It is a simple notification procedure set out under the main EU financial directives (such as CRD IV, MiFID II, UCITS, AIFMD or PSD2), which involves the home Member State notifying the host Member State that the relevant entity intends to provide services in its territory. A fintech authorised as an EU financial service provider under those directives would also have access to the passporting procedure.

For non-EU financial services providers, however, their provision of services in Spain is subject to an authorisation procedure before the BoS, the CNMV or the DGSFP, even if they intend to provide services by means of a branch or from the territory of their home state. A non-EU fintech authorised as a financial services provider would also have access to the same authorisation procedure.

A local licence is not necessary if the entity is passported or authorised to provide its services from its home state into Spain. Additionally, a branch is not strictly necessary as the freedom-to-provide-services option is also possible, although in certain cases Spanish law does not provide such an alternative and the establishment of a branch is a must. The marketing of certain services and products in Spain will be subject to Spanish law and may trigger licensing requirements depending on the circumstances. The unsolicited provision of services does not trigger licensing requirements if no actual services are provided in Spanish territory.

In the case of crowdfunding platforms and in accordance with the Proposal, the authorisation to be granted by the ESMA to a crowdfunding service provider shall be effective for the entire territory of the European Union. Thus, there will be no need to passport a local licence to other Member States for those companies to provide their services in the host Member State. Additionally, the Proposal states that host Member States shall not require crowdfunding service providers to have a physical presence in their territory for them to provide their services on a cross-border basis.

The ownership of non-regulated fintech is not restricted in Spain. Regulated fintech (such as credit institutions, investment institutions and insurance companies) are subject to a significant holdings regime that requires a purchaser of a stake of more than 10 per cent to obtain prior authorisation from the relevant supervisory authority.
III  DIGITAL IDENTITY AND ONBOARDING

Yes, digital identity is recognised in our jurisdiction. Different types of digital identities are regulated under (1) Spanish Law 59/2003, of 19 December, on electronic signatures, as it was amended by Regulation 910/2014 (the Spanish Electronic Signature Law) and (2) Regulation (EU) No. 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (Regulation 910/2014) – jointly known as the Electronic Signature Laws.

Digital identity certificates can be issued by any state or private entity that complies with the regime established in the Electronic Signature Laws. However, the most widely recognised certificates are issued by public institutions (the Spanish National Mint and the Tax Authority). Electronic identity is accessible to all national and non-national persons.

The Electronic Signature Laws set out the different categories of electronic signatures depending mainly on their security features as well as the probative effects corresponding to each category, as well as regulating the characteristics and effects of each of them in Spain. In particular, there are three categories: simple electronic signature, advanced electronic signature and qualified electronic signature, in order of the simplest (with fewer security features) to the most complex, based on a recognised certificate and created by a trustworthy signature creation device, which will entail the use of the highest security features.

The three categories of electronic signature are recognised in Spain as being valid to enter into any contractual relationship or transaction. However, the Electronic Signature Laws only recognise the ‘qualified electronic signature’ as having the same value before a court as a handwritten signature on paper. This does not mean that other types of electronic signature do not have any legal effect. Indeed, an electronic signature may not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures. However, the evidential value of each signature will depend on the strength of the different steps of the contracting process and the security measures that have been used to ensure the identification of the signatory throughout the contracting process.

Fintech companies established as financial services providers are subject to anti-money laundering requirements that establish rules for the identification of clients. Such rules enable a digitised onboarding of the clients in certain cases (for instance, when the client’s identity is certified in accordance with applicable regulations on electronic signatures), and subject to certain requirements.

IV  DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

Collective investment vehicles are mainly regulated under Law 35/2003 of 4 November on collective investment schemes and Law 22/2014 of 12 November on venture capital and other closed-ended investment schemes and management companies of the closed-ended investment schemes. There is no specific law for fintech collective investment vehicles.

As opposed to the rest of fintech, and as indicated in Section II, crowdfunding and crowd-lending platforms are subject to Law 5/2015, which, for the first time in Spain, regulates the activities of these platforms. These activities are currently subject to obtaining an authorisation that is granted by the CNMV (with the intervention of the BoS), but this authorisation regime will probably change as a result of the implementation of the
Proposal. In this regard, the ESMA will be the relevant supervisory authority that may grant authorisations for the provision of crowdfunding and crowd-lending services. Peer-to-peer lending that is not performed through a crowd-lending platform is not regulated in Spain.

Spanish consumer lending regulations are applicable when a fintech is engaged in a credit transaction with a consumer. Loans and financings may be assigned by way of an assignment contract and it is very common to assign entire portfolios of loans. Such loans and financings may only be traded if they are converted into a security, which is assigned to a special purpose vehicle (SPV). Such SPV may then issue securities backed by the credit rights arising from loans. The above is the typical structure in securitisations.

The Spanish legal regime on securitisation was amended by Law 5/2015. The assignment of assets to a securitisation fund should comply with the following requirements:

- the transferor and, as the case may be, the issuer of the securities assigned to a securitisation fund must have audited their annual accounts for the last two financial years prior to the incorporation of the fund, except in certain cases;
- the transferor must disclose in its annual reports the current and future assignment of credit rights that impact each year;
- the assignment of the assets to the fund should be formalised in a contract; and
- the management company of the securitisation fund should submit a document to the CNMV for each asset assignment containing certain information on the assets.

We expect that Law 5/2015 will be further amended as a consequence of the publication of Regulation (EU) 2017/2402 and Regulation (EU) 2017/2401, which lay down a general framework for securitisation and create a specific framework for simple, transparent and standardised securitisation within the European Union.

Under Spanish law the rendering of payment services on a professional basis may only be conducted by entities authorised for such purposes. As indicated in Section II, the BoS is the competent authority to grant this authorisation.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

There is no Spanish regulation on blockchain technology, cryptocurrencies or the issuance of tokens. The European and Spanish regulators are starting to review these activities although there are no legal developments as of today with respect to the qualification of tokens as securities.

ESMA published two statements in November 2017 concerning initial coin offerings (ICOs). The first one contained certain alerts to firms involved in ICOs. ESMA outlines that it is the duty of the firms themselves to consider the regulatory framework applicable to them and meet the relevant regulatory requirements, even if they are from outside the European Union. In this regard, although ESMA did not conclude that the Propectus Directive, the MiFID, the AIFMD and the Fourth AMLD are directly applicable to ICOs, cryptocurrencies and tokens, these may fall inside the scope of such regulations. The second statement was related to the warnings that may be considered by the investors when investing in ICOs, cryptocurrencies and tokens. In February 2018, the European Supervisory Authorities also issued a notice warning investors and consumers about the risks associated with buying cryptocurrencies. In February and September 2018, the CNMV issued its criteria regarding ICOs and cryptoassets in similar terms to that of ESMA.
In parallel, ESMA has been working with different national competent authorities (including the CNMV) to analyse the different business models of cryptoassets, the risks and potential benefits that they may introduce, and how they fit within the existing regulatory framework. Based on this, ESMA issued advice on ICOs and cryptoassets in January 2019. This report identified the gaps in the existing regulatory framework in relation to the ICOs and cryptoassets. We expect further regulation from the EU on the basis of this advice to address the gaps identified by ESMA.

In March 2019, the CNMV issued a statement to clarify that it has neither authorised any prospectus nor authorised or verified any transaction in connection with cryptocurrencies.

The current European and Spanish legislation on anti-money laundering is not directly applicable to ICOs, cryptocurrencies and tokens. However, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLD), contains a provision by virtue of which the AMLD will be applicable to service providers of exchange services between virtual currencies and fiat currencies and custodian wallet providers.

In light of ESMA’s statements, the CNMV and the BoS have also warned firms and investors regarding the regulations and risks inherent to ICOs, cryptocurrencies and tokens.

As concerns the tax treatment of cryptocurrencies and tokens in Spain, the matter is not a clear-cut issue, although the European Court of Justice (ECJ) and the Spanish tax authorities have provided specific guidelines.

Regarding Spanish value added tax (VAT), the judgment of 22 October 2015, Case C-264/14, ruled that transactions involving non-traditional currencies, such as cryptocurrencies, are exempt from VAT pursuant to Article 135(1)(e) of the Council Directive 2006/112/EC, of 28 November 2006, on the common system of VAT. Therefore, in accordance with the ECJ’s considerations, sale and purchase transactions over cryptocurrencies carried out by VAT taxable persons should be exempt from Spanish VAT. On the contrary, ‘mining’ activities to generate cryptocurrencies should not be subject to VAT. Both criteria have also been shared by the Spanish tax authorities in specific binding tax rulings.

For Spanish tax-resident individuals holding cryptocurrencies, and pursuant to specific binding rulings issued by the General Directorate of Taxes in 2018, income triggered upon the sale or transfer of cryptocurrencies (including that resulting from the exchange of one type of cryptocurrency for another) should be deemed as capital gains from a Spanish tax standpoint, and should be taxed accordingly. Specific activities concerning cryptocurrencies (e.g., mining) may have a different tax treatment and, potentially, be deemed as business activities for Spanish tax purposes (income tax, business tax, etc.).

VI OTHER NEW BUSINESS MODELS

Similarly to ICOs, cryptocurrencies and tokens, self-executing contracts are not specifically regulated in Spain and so are permitted and subject to Spanish contract law like any other contract. There are no particular arbitration or mediation schemes for self-contracts. These mechanisms are available in the same terms as for any other contract. Although self-executing contracts lack legislation of their own, we believe the below rules should be taken into account: a should the self-executing contract consist of pre-established clauses imposed by one of the parties for a generality of contracts, Law 7/1998 of 13 April on General Contracting Conditions will apply, which imposes certain conditions and interpretation rules, as well as a public registry for general conditions;
in the event that a self-executing contract is entered into with consumers, Royal Legislative Decree 1/2007 of 16 November approving the revised text of the general law on the protection of consumers and users, would also be applicable. This regulation establishes guiding principles applicable to relationships between consumers and users (understood as legal or natural persons acting in a context that falls outside of their entrepreneurial or professional activities) and entrepreneurs;

also of note is Law 34/2002, of 11 July, on services of the information society and electronic commerce, which would apply in the event that the contract is entered into by electronic means. It establishes a regulatory regime for electronic agreements (e.g., the information to be provided to the contracting parties prior to and after the execution of the relevant agreements, the conditions applicable for the validity of electronic agreements, other obligations applicable to the electronic providers); and

in the event that the contract falls into the definition of a financial service, Law 22/2007 on the distance marketing of financial services addressed to consumers, setting out the rules for electronic agreements and electronic marketing communications, would also be applicable.

Fully automated investment processes are not regulated as such under Spanish law. However, there are provisions within Regulation (EU) No. 595/2014 of the European Parliament and of the Council of 16 April on market abuse (MAR) and Directive 2014/65/EU of the European Parliament and of the Council of 15 May on markets in financial instruments (MiFID II) that refer to algorithmic trading and high-frequency trading strategies.

In addition, third-party websites comparing products or providing information about financial products are subject to general data protection rules, in the same way as other service providers. They are also subject to competition rules, although they are generally not an area of concern for competition authorities to the extent that they favour free competition among the players in the market. However, concerns may be raised in the event that these websites impose most-favoured-nation clauses on any of the players.

From a pure regulatory perspective, the provision of information about financial products is not subject to authorisation provided that this information does not involve the provision of any other regulated services (for instance, investment advice).

In recent years the financial industry has seen a fast-growing adaption of the economy to fintech. The most important sectoral innovations are those related to credit, payment and investment management services. Crowdfunding, crowd-lending and TPPs are good examples of new businesses models.

The insurtech market has also experimented significant growth and, as of December 2019, there are 196 start-ups in Spain related to this business, according to the Insurtech Map of the Spanish Fintech and Insurtech Association. Further disruption is expected in the insurtech market in the near future.

Another new business model that has recently emerged is based on the commercialisation of big data regarding consumer trends based on clients’ data. This model has been already questioned by the Spanish data protection authority, which imposes restrictions on the validity of customers’ consent for their data to be used in an aggregated manner for its commercialisation.

Generally, the main legal and regulatory issues for fintech in Spain are the obstacles resulting from the provision of financial services that trigger licensing requirements. As stated in Section I, the current legal regime for the authorisation of financial entities, which is
Spain

established by reference to EU law, does not provide for a simplified procedure for businesses that only provide a limited range of services, as is the case of many fintech. Hence, as of today, fintech providing regulated services such as payment or investments services must navigate complex and burdensome procedures in Spain or in their country of establishment before having access to customers.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

i Intellectual property

Fintech businesses models and related software may be protected by the rules applicable to the ownership of inventions and works, which should be analysed separately.

Fintech business models may be classed as inventions that are typically the result of research. That result may essentially be protected by patents, utility models or, if such protection is not available or the parties do not wish to request it, inventions can also enjoy a certain degree of protection as know-how or as trade secrets:

- Spanish patents provide protection for inventions for 20 years as of the filing date;
- utility models protect inventions of lower inventive rank than patents, and are granted for a period of 10 years;
- once the referred protection periods have expired, the invention will enter the public domain and may be freely used by any person; and
- know-how has value as long as it is protected as a trade secret and, thus, it is kept confidential (as opposed to patents and utility models), which means that it is not generally known by individuals belonging to the environment where such information would be known and it is not easily accessible by them, it has a potential or effective commercial value by being secret and it has been subject to reasonable measures to keep it secret. These measures could include, among other things, contracts (confidentiality agreements) and the adoption of practical measures (security measures, such as password protection, limitations on access to certain personnel, etc.) demonstrating that the invention or work remains valuable.

On a separate note, software is be deemed an invention but is protected by copyright from the very moment of its creation. Registration is not necessary for the protection of software. The exploitation rights for the work will run for the life of the author and survive 70 years after the author's actual or declared death.

Regarding the ownership of IP rights, the ownership of inventions and works should again be analysed separately. These are default rules under Spanish law to attribute ownership of inventions.

Absent other applicable rules, the natural person who creates the invention (i.e., the inventor) is the owner.

If the inventor is an employee (private or public):

- if the invention is a result of his or her work for a company, pursuant to the terms of his or her employment agreement or to the instructions received from the company, then the owner of the rights to the invention will be the company; and
- if the invention is a result of his or her independent work but relevant knowledge obtained from a company or the company's facilities was used, then the company can claim ownership rights to the invention or a right to use the invention, subject to the payment of fair compensation.
The rule in connection with works is that the original owner of the rights to the work is the author or co-authors (or, in very specific and limited cases, an individual or a legal private or public entity who leads and coordinates personal contributions and publishes the result under its own name – usually in the case of software). The general rule is that the author is the owner of all moral and exploitation rights to the work. However, some specific legal presumptions as well as some important exceptions exist:

a  Regarding copyrightable work created by an employee under his or her employment agreement, Spanish law presumes that, unless otherwise agreed, all exploitation rights of the work have been assigned, on an exclusive basis, to the company for the purposes of its ordinary course of business. This assumption applies in particular, but is not limited to, the creation of software.

b  In the event of joint co-authors, either:

• all co-authors have equal exploitation rights, unless otherwise agreed; or
• the exploitation rights to the work correspond to the (legal or natural) person that assumes responsibility for the creation of the work and publishes it under the person’s own name.

ii  Data protection

Fintech businesses located in Spain or, under certain circumstances, businesses addressing the Spanish market from non-EU territories are subject to data protection rules to the extent that they access and process personal data, either as data controllers or as service providers (i.e., data processors processing the data on behalf of their clients). From 25 May 2018, the main data protection rule applicable in Spain is the General Data Protection Regulation (Regulation (UE) 2016/679) (GDPR) that is directly applicable to all EU Member States. This new legal framework provides some benefits, such as the homogenisation of data protection rules within the EU, which can help local fintech businesses to expand to other EU Member States and may make it easier for fintech businesses from territories outside Spain that are GDPR-compliant to launch their services in the Spanish market.

Notwithstanding the above, at a national level and in addition to GDPR, certain local data protection rules exist in Spain. In particular, a new general data protection law was passed in December 2018: Spanish Basic Law 3/2018 on Data Protection and Digital Rights Guarantees (LOPD). The LOPD formally repealed the previous national data protection regulations, which were incompatible with the GDPR, and adapted local rules in order for them to be compatible with GDPR. The main goal of the LOPD is providing specific data protection regulation in different matters that are not expressly covered by the GDPR or that are covered by the GDPR but in relation to which the Member States are given some competence to enact a more detailed regulation. Consequently, certain data processing (such as inclusion of debtors’ data in creditworthiness shared files) have been regulated in detail in the LOPD. Also, the LOPD has approved a new set of rights of citizens in relation to new technologies, known as ‘digital rights’. This set of new digital rights may impact the business of certain fintech businesses, such as digital rights granted to employees regarding the use by employers of IT tools for monitoring purposes in the workplace or the use of geolocation systems.

Finally, the criteria of the Spanish Data Protection Agency, which is one of the most active data protection authorities within the EU, must also be taken into account.

As regards the possibilities of fintech companies carrying out profiling activities (i.e., the processing of personal data involving the profiling and, in some cases, the adoption of automated decisions with an impact on individuals), such activities are subject to the GDPR
rules and to certain guidelines of the Spanish Data Protection Agency. In general terms, the profiling activities under the GDPR need to be based on lawful legitimate grounds, mainly the existence of a legal duty (e.g., scoring or fraud prevention), the unambiguous or explicit consent of individuals or the existence of a legitimate interest. The interpretation of the Spanish Data Protection Agency of the legitimate interest as a lawful ground for companies to carry out profiling activities has been quite restrictive in the past (e.g., it does not cover profiling carried out with second- or third-party data). Also, additional information and transparency duties must be complied with by fintech companies when carrying out profiling activities. In addition, if AI technologies are used to carry out profiling activities, fintech businesses must take into account the guidelines on AI issued by the Spanish Data Protection Agency. Other additional guarantees, such as reinforced objection rights or the need to carry out privacy impact assessments are imposed. Finally, some of these profiling activities may be carried out with anonymised or pseudo-anonymised data. If this were the case, fintech business must take into account that the Spanish Data Protection Agency has issued specific guidelines for carrying out anonymisation processes.\footnote{Available in Spanish at https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf.}

\textbf{VIII YEAR IN REVIEW}

No specific regulation on fintech was published in the past 18 months except for the implementation in Spain of PSD2, which has come to regulate the activity of TPPs. TPPs are an example of fintech companies that provide payment initiation services or account information services. TPPs must adopt certain security measures when providing their services. Among other obligations, TPPs must ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transferred through safe and efficient channels. Additionally, TPPs must not use, access or store any data for purposes other than for the provision of the payment initiation service. The incorporation of TPPs is subject to the authorisation of the BoS. The initial capital of those TPPs that provide payment initiation services must at no time be less than €50,000. However, if the TPPs only provide account information services, they will not be subject to the initial capital requirement.

Apart from the above, the European Commission issued a public consultation on fintech in March 2017 addressed to all citizens and organisations. The consultation period finalised in June 2017. After the analysis of the responses given, the European Commission has issued an action plan on fintech in March 2018 (the Action Plan).

The Action Plan sets out some steps to enable innovative business models to scale up, support the uptake of new technologies, increase cybersecurity and the integrity of the financial system. In accordance with the Action Plan, the European Commission will, among other things:
\begin{itemize}
  \item[a] host an EU FinTech Laboratory where European and national authorities will engage with tech providers in a neutral, non-commercial space;
  \item[b] present a blueprint with best practices on regulatory sandboxes, based on guidance from European Supervisory Authorities; and
\end{itemize}
report on the challenges and opportunities of cryptoassets later in 2018 in the framework of its EU Blockchain Observatory and Forum, which was launched in February 2018 for a period of two years.

As announced in the Action Plan, the European Commission has established an EU FinTech Lab to raise the level of regulatory and supervisory capacity and to share knowledge about new technologies. The EU FinTech Lab met for the first time on 20 June 2018 in Brussels. The focus of the session was outsourcing to cloud in the banking and insurance sectors. Also they addressed a number of specific questions and challenges around this technology, to enhance understanding and facilitate the work of regulators on cloud outsourcing.

On 13 December 2019, the EU FinTech Lab published its recommendations on how to create a framework for technology-enabled provision of financial services. The EU FinTech Lab’s 30 recommendations pertain to the innovative use of technology in finance, maintaining a level playing field, access to data, and the financial inclusion and ethical use of data.

Additionally, it should be highlighted that Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive) provided legal measures to enhance the overall level of cybersecurity in Member States. Spain incorporated the NIS Directive with the Royal Decree-Law 12/2018, of 7 September, on security of networks and information systems, although the necessary implementing regulations are yet to come.

IX OUTLOOK AND CONCLUSIONS

The fintech sector in Spain is still in the process of significant expansion, mainly in sectors where intermediation between parties is fundamental (e.g., lending, FX, brokerage and investment services such as investment advice and portfolio management) and in the payments sector. Overall, the development of online payment platforms and big data, robotics and artificial intelligence tools represent the most recent trends in innovation (to date, mainly crowdfunding and crowd-lending platforms and robo-advisers). This expansion process is expected to continue in the coming years. This, combined with the increasing interest expressed by European and Spanish regulators in the sector, means that it is likely that fintech will be regulated in the short or medium term.

Apart from that, recent regulatory changes have entered into force in the past months, such as the General Data Protection Regulation (EU Regulation 2016/679), the new law on trade secrets (Law 1/2019) and the LOPD. Although there is no certainty about when the Proposal could be passed by the European Parliament and the Council, and when the Draft Bill will be passed by the Spanish government, they should be taken into consideration owing to their impact on the fintech legal framework.

Apart from the above, the main disruption in the global financial sector is still expected to result from ledger technologies such as blockchain. Although the use of this type of technology is not yet widespread, it is expected to emerge in Spain in many areas and will not just be limited to cybersecurity and cryptocurrencies.
Chapter 23

SWITZERLAND

Thomas A Frick

I OVERVIEW

The approach taken in Switzerland to fintech continues to be a supportive and positive one, both by the government and by the ecosystem. Although no separate financial regulatory regime exists for fintech companies, the existing rules are applied in a way that enables a lively fintech scene to grow. Furthermore, rules were and are about to be changed to enable, for example, crowdfunding to operate more effectively, banks to do a fully digital onboarding of clients, financial institutions to experiment with new business models and to adapt civil and bankruptcy laws to cryptoassets. The Swiss Financial Markets Supervisory Authority (FINMA) set up a special fintech desk and declared that it intends to structure regulation in a technology-neutral way. The Swiss government initiated a Crypto-Initiative and set up a working group for blockchain and initial coin offering (ICOs) in January 2018, which led to a comprehensive report in December 2018 and a proposal for focused changes to existing laws to the parliament in November 2019. For example, in the canton of Zug, even taxes can be paid in Bitcoin.

A summary of the regulatory framework as in force today can be found on FINMA’s website.2 Regular updates on developments are available on a (private) site.3

The regulatory framework (equally applicable to any other financial service provider in Switzerland) is particularly based on the Federal Act on Banks and Savings (the Banking Act), the new Financial Institutions Act (FIA) that became effective on 1 January 2020, the Anti-Money Laundering Act (AMLA), the Collective Investment Schemes Act (CISA) and the Financial Market Infrastructure Act (FMIA). In addition, provisions of the Federal Act on Data Protection (FADP), the Consumer Credit Act (CCA) or the Federal Act against Unfair Competition (UCA) may be applicable. FINMA and the Swiss Federal government have on various occasions emphasised that they regard innovation as a key for the Swiss financial centre and encourage digitalisation as well as technological advancements. FINMA holds regular fintech roundtables and has designated a team as fintech desk to be the contact point for fintech companies (however, it also set up a dedicated fintech team in its enforcement department, and initiated a number of investigations in particular against ICOs).

There is also no separate tax law system applicable to fintech companies in Switzerland. Fintech projects and investments in digital currencies and tokens are therefore taxed like any other traditional investment vehicle. However, the tax administration declared that, for example, Bitcoin will be treated like a foreign currency for tax purposes, so that no value

---

1 Thomas A Frick is a partner at Niederer Kraft Frey.
2 https://www.finma.ch/de/bewilligung/fintech/.
3 http://fintechnews.ch/.
added tax is levied. Cantonal tax administrations have published a number of guidelines on how cryptocurrencies are treated for tax purposes. As the Swiss tax authorities are willing to issue tax rulings, fintech projects can obtain a ruling and thereafter operate with certainty about the tax regime applicable to them.

Overall Switzerland can be considered (and is internationally recognised) as a very fintech-friendly jurisdiction, despite the fact that no fintech specific regulation or tax regime exists. Many fintech start-ups and projects show that the legal environment is considered as advantageous. Currently, the main impediment for fintech projects in the field of cryptoassets continues to be to find suitable partners in the traditional finance industry, although the number of crypto-brokers and exchange projects is increasing, and despite the Swiss Bankers Association issuing guidelines for the opening of bank accounts for crypto-projects in 2018. However, this hardly limits the numerous projects for security tokens or applying artificial intelligence (AI) in the finance industry.

II REGULATION

i Licensing and marketing

Under Swiss law, no specific fintech licence exists at present, as Swiss regulation is technology-neutral and principle-based. Nonetheless, a fintech company may be subject to a licence or ongoing compliance and reporting obligations. Some forms of financial business activities are prudentially supervised by FINMA on an ongoing basis and require a licence granted by FINMA, while others only have to join one of Switzerland’s self-regulatory organisations that were set up to ensure compliance with anti-money laundering requirements. The regulations of these self-regulatory organisations (SROs) are recognised by FINMA as a minimum standard for anti-money laundering (AML) compliance.

Depending on their business model, fintech companies are particularly likely to fall within the scope of the Banking Act, the FIA and the AMLA.

Banking Act

According to the Swiss Banking Act, anyone who accepts ‘deposits from the public on a commercial basis’ is subject to banking licence requirements. This is the case if either:

a deposits of more than 20 investors are actually held; or

b the person or entity publicly announces to a non-limited number of persons that it is willing to accept such funds (regardless of the final actual number of investors).

Thus, fintech companies that accept or raise funds stemming from the public, such as crowdfunding or ICOs, may fall under bank licence requirements. Bond issues do not qualify as deposits, and capital contributions that do not entail a repayment obligation also do not qualify as deposits, which is why ICOs are possible – under certain conditions – under Swiss law.

In order to better accommodate Swiss fintech projects, the Swiss government (the Federal Council) in 2017 amended the Ordinance on Banks and Savings Banks (the Banking Ordinance) to include exemptions from the requirement to obtain a licence. As from 1 August 2017, the holding of client funds (of more than 20 investors and for a period longer

4 Article 1 Paragraph 2 Banking Act.
than 60 days) no longer triggers banking licensing requirements (as it is no longer deemed to meet the requirement of ‘on a commercial basis’) if certain requirements are met. These requirements are:

a. the funds do not at any time exceed 1 million Swiss francs;
b. the funds are neither reinvested nor interest-bearing (with exceptions); and
c. the depositors have been informed in writing or otherwise in text form prior to making the deposits that their funds are not covered by the Swiss depositors protection regime and that the institution is not supervised by FINMA.

With regards to (a), the threshold will be calculated on the basis of the aggregate deposits held at any given period.

In addition, funds on settlements accounts may be held for 60 days (previously only seven days) if they are not interest-bearing.\(^5\) This provision in particular aims to allow crowdfunding companies to hold assets for a longer period without requiring a banking licence.

Furthermore, on 1 January 2019, a special licence was introduced: undertakings accepting deposits from the public of up to 100 million Swiss francs, but not paying interest on such deposits, may qualify for a ‘banking licence light’ – a licence that subjects such undertaking to rules less stringent than the rules applicable to banks.\(^6\) This new licence is often referred to as a fintech licence, although it is not only available to fintechs.

**FIA**

A licence from FINMA is required in order to act as a securities house.\(^7\) A securities house is any natural person or legal entity or partnership that commercially buys and sells securities on the primary market for their own account for short-term resale or for the account of third parties, offers them publicly on the primary market or even creates or publicly offers derivatives.\(^8\) The term ‘securities’ is now defined in the FMIA and means, in accordance with Article 2 Lit. b FMIA, ‘standardised certificated and uncertificated securities, derivatives and intermediated securities, which are suitable for mass trading’. Further clarification is provided by Article 2 of the Ordinance on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading, which states in Paragraph 1:

> Securities suitable for mass standardised trading encompass certificated and uncertificated securities, derivatives, and intermediated securities which are publicly offered for sale in the same structure and denomination or are placed with more than 20 clients, insofar as they have not been created especially for individual counterparties.

Therefore, for trading tokens it is relevant whether these are qualified as securities within the meaning of FIA and FMIA (see below, on ICOs).

---

5. Article 5 Paragraph 3 Lit. c Banking Ordinance.
6. Article 1a and 1b Banking Act.
7. Article 2 Paragraph 1 FIA.
8. Article 41 FIA.
AMLA

Even if neither a banking nor a securities house licence is required, AML regulations and provisions may apply. Swiss AML regulations apply to institutions that are considered per se as financial intermediaries (e.g., banks, securities houses, fund management companies and insurances) and institutions that engage in a ‘financial intermediary activity (e.g., asset managers, investment advisers with power of attorneys). If a fintech company is engaged in financial intermediary activity, it is required to join a recognised Swiss AML SRO or submit to direct supervision by FINMA on AML matters, and needs to comply with the applicable AML duties (such as identification of customer, establishment of beneficial ownership). Some of the AML duties entail sanctioning provisions under criminal law, and such provisions are equally applicable to fintech companies. Under a recent proposal of the Federal Council, the applicability of AML rules to fintech companies will be further specified and enlarged. In its supervisory notification 02/2019 of 26 August 2019, FINMA held that token transfers require identification of the recipient and its beneficial owner, without a minimum threshold applying. Switzerland has, therefore, one of the strictest AML regimes regarding token transfers.

Further rules

Fintech companies may market their products and services under the same rules as established financial service providers. Restrictions apply in particular if a company looks for funds and contacts more than 20 potential investors (see above).

If an institution were to set up an automated digital advisory service in Switzerland, the same licence requirements would apply as for any other institution offering non-digital advisory services. A ‘pure’ investment advisory service without any power of attorney over clients’ accounts is not subject to licence requirements (but is subject to behavioural rules similar to the Markets in Financial Instruments Directive under the new Financial Services Act (FinSA) that became effective on 1 January 2020). An investment advisory service with a power of attorney also requires a licence under the FIA, since 1 January 2020.

Credit information services may be provided subject to the FADP; under current Swiss law, this Act applies not only to persons but to legal entities as well, so that any information about corporate credit ratings may fall under the scope of the Act. The Act is about to be changed and will most likely no longer apply to legal entities in the future.

ii  Cross-border issues

As Switzerland is not a member of the European Union, regulated or licensed activities may not be passported into Switzerland. Holding a licence abroad may sometimes make a licensing process in Switzerland more cumbersome, as FINMA may reach out to the foreign authority in order to find an agreement on consolidated supervision, which may prove to be a lengthier process.

Companies that provide services to clients in Switzerland on a pure cross-border basis (cross-border inbound) without physical presence may require a licence in certain instances. The distribution of collective investment schemes is permitted only if done by reverse solicitation, namely, on the initiative of the investor itself. The same applies with respect to insurance products. Both collective investment schemes and insurance products are subject to strict rules on marketing. Under the FinSA, client advisors of foreign financial intermediaries may only become active in Switzerland if they are registered in the Swiss client advisors register.
A service provider is deemed to have physical presence in Switzerland if it has a branch or similar formal presence in Swiss territory, or the presence of individual persons in Swiss territory on a permanent basis who are employed or mandated by licensee to act on its behalf. The term ‘on a permanent basis’ means having individuals permanently on the ground in Switzerland, or individuals who frequently travel to Switzerland for the purpose of carrying out sales or marketing activities in Switzerland. FINMA has not published guidance on what constitutes frequent travel; whether travel is frequent is assessed by evaluating all relevant facts and circumstances (i.e., frequency of travel, number of persons traveling to Switzerland, etc.). FINMA has substantial discretion when assessing whether physical presence is established in Switzerland.

There are no Swiss laws of general application prohibiting or subjecting to prior approval foreign investments in Switzerland. Therefore, foreign investors do not generally need formal approval for their investments in Switzerland and no special governmental authority monitors them. Foreign investments in certain regulated industries might require governmental permission. If foreign nationals have a controlling influence on a bank, a securities trader or certain other prudentially supervised entities active in the financial sector (a finance company), the granting of a respective licence by FINMA is subject to certain additional requirements. Investment restrictions also apply to the acquisition of residential (but not commercial) real estate in Switzerland by foreign or foreign controlled persons and under the Telecommunications Act for radio communication licences, under the Nuclear Act for nuclear power plants, under the Radio and Television Act for broadcasting licences and under the Aviation Act for the professional transport of passengers or goods.

Switzerland does not have currency controls in place. Hence, both investments and repatriation of the capital and profits are possible.

III  DIGITAL IDENTITY AND ONBOARDING

There is currently no generally recognised digital identity in Switzerland. However, various efforts have been undertaken to raise digital awareness in Switzerland and to introduce a generally recognised digital identity. On 22 February 2017, the Federal Council presented a draft for a Federal Act on Recognised Electronic Identification (the E-ID Act), which was approved by the first chamber of parliament in March 2019. Under the E-ID Act, private providers (supervised by the federal administration) would be authorised to issue recognised digital identities. On 22 November 2017, two private project groups (one from the Swiss Federal Railway and the Postal Services; the other from the former state telecom and the two major banks UBS and Credit Suisse) announced that they will join forces and set up such a private provider under the name of Swiss-Sign. It is expected that this will lead to the establishment of a broadly accepted Swiss E-ID, available not only to nationals but also to non-Swiss citizens; however, the details of the limitations are still subject to discussions.

Switzerland has known for some time already the electronic signature that guarantees the authenticity of a document, a message or other electronic data and ensures the identity of the signatory.

Since 2016, financial service providers may carry out fully digitised onboarding of clients. On 17 March 2016, FINMA published Circular 2016/7 ‘Video and Online Identification’, which entered into force on 18 March 2016 (revised in 2018) and stipulates
AML requirements with regard to the onboarding process of clients via digital channels. The circular applies directly to financial intermediaries. Subject to adherence to specific requirements, financial intermediaries may onboard clients by means of video transmission.

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i Collective investment schemes
Collective investment schemes governed by CISA are assets, raised from investors for the purpose of collective investment, which are managed for the account of such investors, whereby the investment requirements of the investors are met on an equal basis. Open-ended collective investment schemes are organised under company or contract law; closed ones only under company law.

ii Crowdfunding
Under Swiss law, crowdfunding is permitted and does not per se trigger a licence requirement. However, if crowdfunding includes ‘assets raised from investors for the purpose of collective investment’ and these crowdfunding assets are managed for the account of such investors (by a third party), subject to equal treatment provisions, they would qualify as collective investment scheme within the meaning of CISA. In such case, the respective requirements according to CISA would have to be adhered to.

iii Crowd-lending
Crowd-lending, also known as peer-to-peer lending, is not per se regulated. However, depending on its specific set-up, it may fall within the scope of the Banking Act, FIA, AMLA, etc. In addition, a consumer credit agreement is a contract whereby a creditor grants or promises to grant credit (not exceeding 80,000 Swiss francs) to a consumer in the form of a deferred payment, a loan or other similar financial accommodation. In general, the CCA will be applicable to crowd-lending activities if the counterparty were to qualify as a consumer. In such case, the respective rules of the CCA would have to be adhered to, for example, the maximum interest possible for consumer credits currently amounts to 10 per cent.

Platforms providing crowdfunding and crowd-lending services do not require a licence if the funds of the investors are directly sent to the projects (i.e., not through the platform). If funds are sent via accounts of the platform, this can only be done without a banking licence if the account is non-interest-bearing, the funds are kept not longer than 60 days on the account and the client is informed that the platform does not hold a licence. The platform will need to register as a financial intermediary with an SRO and to comply with AML obligations.

Even the project developer may qualify as a bank if it accepts more than 20 loans and the amount exceeds 1 million Swiss francs.

9 Article 7 Paragraph 1 CISA.
10 Article 1 Paragraph 1 CCA.
11 Article 14 CCA and Article 1 of the Ordinance on the Consumer Credit.
Loans can be traded on secondary markets, subject to compliance with AML laws. However, the transfer of a loan requires either transfer of the contract or assignment of the claim. Assignment of claims can only be done in writing; in other words, with a handwritten (or electronic) signature of the assignor.

iv Payment systems
Payment systems only require a licence from FINMA if they are deemed relevant for the proper functioning of the financial market or for the protection of financial market participants and if the payment system is not operated by a bank. As a rule, payment systems are not deemed relevant and can be operated without licence; however, in the Libra project, FINMA stated that it considers the project as a relevant system requiring a licence. In order to be eligible for a FINMA licence as a payment system, certain requirements have to be met. For example, the applicant must be a legal entity under Swiss law and have its registered office and head office in Switzerland, provide for a guarantee of irreproachable business conduct, the minimum capital of the applicant must be fully paid in and the applicant must possess appropriate IT systems.

Switzerland not being a member of the European Economic Area, it decided not to implement the second Payment Services Directive of the EU. This means that there is no harmonisation of interfaces and no general access to accounts for third-party payment service providers must be granted by Swiss banks. However, as banking services in Switzerland are often cross-border, it is expected that many banks will soon provide open access to account interfaces upon request of their clients.

v Digital marketplaces
There are a number of projects to set up digital marketplaces in Switzerland. Up to now, digital marketplaces have existed only for payment tokens, not for security tokens. However, the main Swiss exchange SIX is working on a project.

Under the new DLT Act, it is proposed to change the FMIA to introduce a special licensing category for trading systems for distributed ledger technology (DLT) securities. Such DLT trading systems may offer direct access to individuals (and not only to licensed entities) and shall have the right to offer not only trading, but also central depositary and payment system services (but may not act as central counterparties).

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS
Switzerland does not (yet) have a specific regulation for blockchain technology. Blockchain projects fall under the regulatory regimes of the industries they are applied to, such as the finance industry. Cryptocurrencies caught the attention of the Swiss regulator early: in June 2014, FINMA published a fact-sheet on Bitcoin and confirmed that Bitcoins qualify as currency (i.e., that payments with Bitcoin do not require a licence). Soon, Switzerland and in

---

12 Article 4 FMIA.
13 Article 8 FMIA.
14 Article 9 FMIA.
15 Article 12 FMIA.
16 Article 14 FMIA.
particular the ‘Crypto Valley’ in the canton of Zug established itself as one of the world’s hubs for ICOs, in particular through the Ethereum ICO from July to September 2014. Thereafter, there were a number of high-profile ICOs that caught the attention of the fintech world. At the time, FINMA did not provide specific guidance, although its fintech desk was willing to grant negative clearance to projects submitted.

On 16 February 2018, FINMA published the ‘Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)’ (the ICO Guidelines), wherein it describes in some detail how it deals with the supervisory and regulatory framework for ICOs under Swiss law. It does so by outlining the principles on which it will base its response to specific enquiries, and by providing a checklist of information required to be submitted in an application for negative clearance. These ICO Guidelines are available electronically on the FINMA website, and were amended on 11 September 2019 to more specifically address stablecoins.17 The ICO Guidelines provide some guidance on regulatory matters but do not deal with issues of civil or criminal law. Hence, specific legal advice continues to be needed for any ICO or security token offering (STO).

A key message given by the ICO Guidelines is that FINMA continues to be ready to review ICOs and STOs and to give negative clearance, as far as regulatory aspects are concerned. When reviewing a project, FINMA will consider, among other things, not only the investor categories an ICO targets, compliance with AML regulations, and the functionalities of the token generated including the rights it confers to the investor, but also the technologies used (distributed ledger technologies, open-source, etc.), the technical standards (such as the Ethereum ERC20) and the wallets and technical standards to transfer tokens.

FINMA distinguishes three token categories:

a payment tokens (i.e., cryptocurrencies), which are intended to be used as a means of payment and do not grant any claims against the issuer of the token;

b utility tokens, which grant access to an application or service; and
c asset tokens, which represent assets such as a debt or equity claim against the issuer, or that enable physical assets to be traded on the blockchain.

If a token combines functions of more than one of these categories, it is considered a hybrid token and has to comply with the requirements of all categories concerned.

To assess whether tokens qualify as securities under Swiss law, FINMA applies the general definition of the Swiss Financial Market Infrastructure Act. For the time being, FINMA will not consider payment tokens to be securities; utility tokens will only be considered securities if they have an investment purpose at the point of issue. Asset tokens will be considered as securities.

FINMA confirms that the creation of uncertificated securities and their public offering are not regulated, unless they qualify as derivative products. However, underwriting and offering (in a professional capacity) security tokens of third parties publicly on the primary market is a licensed activity. Furthermore, the issuing of tokens that are similar to bonds or shares may trigger prospectus requirements.

FINMA confirms that the issuing of tokens will not qualify as deposits; in other words, it does not require a banking licence, unless the tokens grant claims with debt capital

character against the issuer (for that reason, FINMA took action against Envion). Collective investment schemes regulations may apply if the funds received by an ICO are managed by third parties.

Issuing payment tokens will trigger the application of the anti-money laundering act (AMLA) provisions, if the tokens can be transferred technically on a blockchain infrastructure. Issuing utility tokens will not trigger such application, as long as their main purpose is providing access to a non-financial application of the blockchain technology. Asset tokens are not deemed a means of payment under the AMLA. FINMA clarifies that the application of the AMLA will not only be triggered by an exchange of a cryptocurrency against a fiat currency, but also by an exchange against a different cryptocurrency.

Rights granted in the pre-sale phase are considered as securities by FINMA if they are standardised and suitable for mass standardised trading. If so, they are not subject to AML regulations.

There are numerous private initiatives to provide market guidance and to establish standards. On 8 January 2018, the Crypto Valley Association, an independent, government-supported association established to support fintech institutions in the canton of Zug, published a General Code of Conduct that aims to subject its members to a minimum standard with regards to transparency and information when conducting an ICO. On 21 September 2018, the Swiss Bankers Association published guidelines on the opening of corporate accounts for blockchain companies (with and without ICOs), which aim to promote a diverse fintech ecosystem, at the same time securing the integrity of the Swiss financial market.

To further tokenisation of assets, both the Crypto Valley Association on 15 December 2019 and the capital markets and technology association (in October 2018) published guidance papers on asset and share tokenisation. One of the key aspects is whether security tokens can be validly transferred on the blockchain. Both organisations argue that this is indeed the case today. Further clarification and legal certainty will be provided by the new Blockchain Act (see Section XI below) that stipulates that shares and bonds can be issued in tokenised form and that tokens can be transferred on the blockchain. Other assets such as real estate are usually held by an SPV that issues the token.

There is no separate tax regime applicable to digital currencies and tokens. Cryptocurrencies and tokens are therefore taxed like any other traditional investment vehicle. However, on most tokens, no VAT, no issuing tax and no withholding tax is levied when the token is issued, subject to certain exceptions. Swiss residents do not pay taxes on capital gains of privately held assets.

Tokens may be offered to Swiss residents from outside of Switzerland, but are subject to similar requirements as applicable to tokens issued in Switzerland, namely, they may not qualify as derivative products, security tokens may not be offered by a third party in a professional capacity and tokens that are similar to bonds or shares may trigger prospectus requirements.

VI OTHER NEW BUSINESS MODELS

Self-executing contracts are generally permitted by Swiss law, as long as the essential terms and conditions of the contract are agreed upon by both parties. Fully automated investment processes such as robo-advisers are not per se prohibited by Swiss law, as long as the clients concerned are informed and agreed respectively.
AI projects are not separately regulated and they need to comply with the regulations applicable to the actual project. In addition to data protection and confidentiality issues regarding the access to data to train self-learning systems, a focus of the current discussion is on compliance and liability. Various compliance rules stipulate that a regulated entity must be aware of and control its decision parameters (e.g., risk management) which may be difficult in deep learning systems. Furthermore, liability issues are unsolved in case of non-controlled deep learning through neuronal networks. A number of insurance companies experiment with new insurtech products, for example, in the field of claims management, customer handling or AI applications in risk assessment. The international Blockchain Insurance Industry Initiative B3i is domiciled in Zurich.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Fintech and software may be protected under patent law or copyright law, depending on the specific details of the technology or software. Unlike in the EU, there is no specific protection of the creator's rights in a database. However, databases and software may be protected under copyright law, if and to the extent they are intellectual creations with individual character with regard to their selection and arrangement. To qualify for patent law protection, a technology or software must be an invention that is new and applicable in the industry, and that solves a technical problem (which is usually not the case in standard software). A technical reproduction process of someone else's market-ready work is prohibited.18

If an employee creates a computer program in the course of discharging professional duties or fulfilling contractual obligations, the employer alone shall be entitled to exercise the exclusive rights of use. Inventions and designs produced by the employee alone or in collaboration with others in the course of his or her work for the employer and in performance of his or her contractual obligations belong to the employer, whether or not they may be protected. By written agreement, the employer may reserve the right to acquire inventions and designs produced by the employee in the course of his or her work for the employer but not in performance of his or her contractual obligations. Business models, as a rule, cannot be subject to intellectual property rights under Swiss law.

Under the Swiss Data Protection Act, protected data are not only data relating to persons but equally data relating to legal entities. Personal data must be protected against unauthorised processing by adequate technical and organisational measures. Processing of data is any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data. Thus, merely providing information or comparing products on a website may fall within the scope of Swiss data protection law (unless the data are public). In addition, such a comparison may be considered unfair under the UCA if the services, prices or business situation were reduced by incorrect, misleading or unnecessarily infringing statements. The storage of personal data on a server in Switzerland may be sufficient to trigger application of Swiss data protection law.

Digital profiling may be considered as a personality profile or even include sensitive personal data within the meaning of the data protection act; in other words, a collection of data that permits an assessment of essential characteristics of the personality of a natural

---

18 Article 5 lit. c UCA.
person. Consent must be expressly given before processing such data and personality profiles (and sensitive personal data) must not be disclosed to a third party without justification. In addition, the data processor must inform the person concerned of:

\( a \) the controller of the data file;
\( b \) the purpose of the processing; and
\( c \) the categories of data recipients (if disclosure were planned).

The Swiss Data Protection Act is under review and it is expected that a revised Act aligned to the EU General Data Protection Regulation will become effective by 2021; however, there may be delays.

VIII YEAR IN REVIEW

The past 18 months were another intense phase for Swiss fintech regulations.

While the ICO boom of 2017 is history and the 2018 infrastructure projects (crypto-brokers, trading places, wallet and storage providers) started to mature, 2019 was expected to be the year of the security tokens offerings. This has not (yet) happened, but numerous other business project were initiated and received funding. Probably the best known of these projects is Facebook’s Libra project. Facebook intended to issue a stablecoin based on a basket of currencies through an association based in Geneva, Switzerland. In a preliminary assessment, FINMA stated that it considered Libra to be a system-relevant payment system requiring a full licence. The project has not progressed further yet.

However, in the summer of 2019, the first two banking licences were issued to crypto banks in Switzerland (SEBA and Sygnum). Additional applications for further licences are pending. It is expected that this will give a boost to the industry that in 2018 complained about lack of access to the traditional financial markets. Another development is that the major Swiss exchange SIX set up a consortium to establish a crypto-based exchange in Switzerland.

On the regulatory side, the dominant theme was the draft of the federal act on adapting the federal law to developments of the DLT (the Swiss DLT Act) published for consultation in March 2019 (on the basis of a comprehensive report published in December 2018). Consultation results were incorporated and the Swiss Federal Council approved a proposal to the parliament in November 2019. The act does not attempt to set up a comprehensive new regulatory system for cryptoassets, but rather comprises numerous but in each case limited changes to existing laws, thereby making the integration of the new rules into the overall legal framework easier.

The proposal focuses on security tokens which are to be regulated as intermediated securities under security law, debt enforcement law and international private law. The proposal privileges such tokens in case of bankruptcy of the wallet holder, thereby limiting the risks of the investors. The proposal clarifies the legal nature of security tokens under Swiss law, including permitted forms for transferring them, and the use of tokens as collateral.

Furthermore, a new financial market infrastructure is proposed – the DLT trading system, which may combine the functions of a trading platform, a depositary and a payment system (but not as a central counterparty) (see above). Additional rules are provided for banks that accept cryptoassets in deposits.

In the revised FINMA-AML Ordinance (changes to which were initiated in June 2018), additional duties of review were introduced for issuers of means of payment (such
as payment tokens); the revised ordinance became effective on 1 January 2020. In its supervisory notification 02/2019 of 26 August 2019, FINMA held that token transfers require identification of the recipient and its beneficial owner, without a minimum threshold applying. Switzerland has, therefore, one of the strictest AML regimes regarding token transfers.

Finally, as mentioned before, the Swiss financial market regulatory regime was amended in a fundamental and comprehensive way with the introduction of the FinSA and the FIA as of 1 January 2020, bringing it closer to the EU regulatory framework.

IX OUTLOOK AND CONCLUSIONS

It is expected that the act on establishing a legal and a distribution framework for a generally accepted digital identity may be finalised by the end of 2020; discussion is ongoing in the parliament. The main matter for debate is that private institutions will issue the digital identity, although based on a state licence.

The draft of the new Data Protection Act published in 2017 is still on hold. The earliest date for it to become effective is in 2021.

The proposal of the DLT Act will be discussed in 2020 in the parliament. It is still possible that at least parts of it become effective by 2021.

While regulatory changes may take more time than expected, there continue to be numerous private and public initiatives that focus on establishing a fintech ecosystem in Switzerland. Among others, the Swiss FinTech Innovation Lab at Zurich University brings together researchers from banking and finance, business informatics, management, social sciences, etc. The university is in the process of establishing 18 new chairs for digitalisation topics.

The focus in 2020 will continue to be on asset tokens: the first projects to tokenise shares and bonds are operative. In addition, there are various insurtech projects, projects to facilitate client onboarding and compliance improvements (regtech) and, in particular, numerous projects to use artificial intelligence in the financial sector. Hence, the environment will remain very dynamic and it can also count on continued support by the industry, various associations and the Swiss and cantonal governments.
Chapter 24

TAIWAN

Abe T S Sung and Eddie Hsiung

I OVERVIEW

In recent years, Taiwan has adopted various initiatives to facilitate financial innovation with the development of technology. In particular, the Financial Supervisory Commission (FSC), Taiwan’s financial regulator, published the ‘Fintech Development Strategy Whitepaper’ in May 2016 to demonstrate its commitment to fintech. In addition, an action plan designed by the FSC to develop Taiwan’s financial sector was later unveiled in June 2018. The plan aims to spur financial innovation and implement a range of financial policies to respond to financial service demands.

Also, to promote fintech services and companies, the Taiwan government promulgated a law for the fintech regulatory sandbox, the FinTech Development and Innovation and Experiment Act (the Sandbox Act), on 31 January 2018, which took effect on 30 April 2018. The Sandbox Act was promulgated to enable fintech businesses to test their financial technologies in a controlled regulatory environment.

There are currently no tax incentives specifically provided for fintech companies.

II REGULATION

i Licensing and marketing

No special fintech licence

In Taiwan, conducting finance-related activities generally requires a licence from the FSC. However, there is no special licence specifically targeted at fintech companies. Depending on the types of regulated activities, fintech companies must meet certain qualifications as required under relevant laws and FSC regulations.

Local marketing rules

The Financial Consumer Protection Act (FCPA) and its related regulations provide for the general marketing rules applicable to marketing materials for financial services. In general under the FCPA, when carrying out advertising, promotional or marketing activities, financial services providers should not falsify, conceal, hide or take any action that would mislead financial consumers, and should ensure the truthfulness of the advertisements.

In addition to the general marketing rules under the FCPA, financial service providers may also be subject to additional marketing rules as specified in the laws and regulations governing specific types of financial services or products.

---

1 Abe T S Sung is a partner and Eddie Hsiung is an associate partner at Lee and Li, Attorneys-at-Law.
Automated digital advisory

Although no special fintech licence exists that is specifically targeted at fintech companies, some guidelines and operating rules have been introduced in recognition that traditional licence requirements do not address fintech. For example, the FSC has approved the ‘Operating Rules for Securities Investment Consulting Enterprises Using Automated Tools to Provide Consulting Service (Robo-Adviser)’ (the Robo-Adviser Rules) issued by the Securities Investment Trust and Consulting Association of Taiwan, Taiwan’s self-disciplinary organisation of the asset management industry. Pursuant to the Robo-Adviser Rules, licensed securities investment consulting enterprises may provide online securities investment consulting services by using automated tools through algorithms (Robo-Adviser Services), and must comply with certain rules including, among others:

- there should be a periodical review of the algorithm;
- relevant know-your-customer procedures should be conducted before provision of advice;
- a special committee should be established to supervise the adequacy of the Robo-Adviser Services; and
- the customers should be informed of precautions before using Robo-Adviser Services.

Credit information service

Pursuant to the Banking Act and relevant regulations, an entity collecting credit-related information from financial institutions, processing such information and maintaining the relevant database and providing credit-related information and records to financial institutions for credit checking purposes must obtain prior approval from the FSC. Currently, the Joint Credit Information Center (JCIC) is the only FSC authorised entity that offers such services. In practice, a bank would normally review the credit information or records provided by the JCIC as part of the bank’s credit investigation on an applicant for a credit extension.

If an entity is not considered as offering such services, no FSC approval is required, but it will still be subject to the Personal Data Protection Act (PDPA) regarding its collection and use of any personal data.

ii Cross-border issues

There is no concept of a ‘passporting right’ in Taiwan. To engage in regulated financial activities, a company needs to apply for the relevant licences to the FSC. As mentioned above, depending on the types of regulated activities, the applicant must meet certain qualifications as required under relevant laws and FSC regulations. Also, under current financial laws and regulations, no person is allowed to provide any financial services in Taiwan without obtaining prior approval or a licence from the FSC.

As for foreign exchange-related restrictions, for each calendar year, a Taiwanese company may, upon filing a report with the Central Bank of the Republic of China (Taiwan) (the Central Bank), purchase foreign currency with Taiwan dollars and remit the foreign currency out of Taiwan for purposes other than trade or service-related payments, in an amount up to US$50 million or its equivalent without special approval from the Central Bank. Foreign exchange purchase for purposes other than trade or service-related payments exceeding the applicable ceiling would require special approval from the Central Bank. Such approval is discretionary and is decided by the Central Bank on a case-by-case basis.
III DIGITAL IDENTITY AND ONBOARDING

Taiwan’s Ministry of Interior has developed a mechanism called the Citizen Digital Certificate. With such Certificate, certain types of governmental applications may be submitted and handled online, without the need to go to the government’s physical office in person. For example, certain tax filings may be done with such certificate. However, such certificate may not be considered a generally recognised digital identity in Taiwan.

However, the Minister of the National Development Council, a policy-planning authority of Taiwan, announced in 2018 that in order to promote digital transformation in Taiwan and elevate the efficiency of public services, the Taiwan Digital ID Card will be distributed in the second half of 2020. However, the exact details of the policy are not yet confirmed.

With regard to digitised onboarding of clients, a customer is generally required to be present at the physical location of a bank in order to open a bank account with such bank for the first time, while there are certain financial services that may be purchased purely online (e.g., certain types of insurance policies).

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i Digital marketplaces

Except for certain rulings and regulations governing security tokens (i.e., the STO Rules as defined and explained below) and anti-money laundering (as further explained below), no Taiwanese laws or regulations have been specifically promulgated or amended to formally regulate digital assets, cryptoassets or their marketplaces.

The issuing, trading and possessing of security tokens is governed by the STO Rules (as defined below), though the current regulatory regime of Taiwan imposes no restriction or prohibition on owning or possessing cryptoassets without the nature of securities or any other financial products of services.

ii Collective investment scheme

Local funds (securities investment trust funds)

The most common form of collective investment scheme in Taiwan is securities investment trust funds, which may be offered to the general public or privately placed to specified persons. Public offering of a securities investment trust fund needs prior approval or effective registration with the FSC or the institution designated by the FSC. No prior approval is required for a private placement of a securities investment trust fund; however, it can only be placed with eligible investors and within five days of the payment of the subscription price for initial investment offering. A report on the private placement should be filed with the FSC or the institution designated by the FSC. Under current laws and regulations, public offering and private placement of securities investment trust funds may only be conducted by FSC-licensed securities investment trust enterprises (SITEs). Currently, the paid-in capital of a SITE should not be lower than NT$300 million, and certain qualifications exist for the shareholders of a SITE. A fintech company that is not a SITE will not be able to raise funds in the same way as a SITE.
**Offshore funds**

Offshore funds with the nature of a securities investment trust fund may also be publicly offered (subject to FSC prior approval) or privately placed (subject to post-filing with the FSC or its designated institution) to Taiwan investors, subject to certain qualifications and conditions. An offshore fintech company that does not have the nature of a securities investment trust fund will not be able to be offered in Taiwan.

**Crowdfunding**

The following two ways of fundraising are generally known as the equity-based crowdfunding platforms in Taiwan. Such ways of crowdfunding are exempted from the prior approval or effective registration normally required under the Securities and Exchange Act (SEA).

**The ‘Go Incubation Board for Startup and Acceleration Firms’ of the Taipei Exchange**

The Taipei Exchange (TPEx), one of the two securities exchanges in Taiwan, established the Go Incubation Board for Startup and Acceleration Firms (GISA) in 2014 for the purpose of assisting innovative and creative small non-public companies in raising capital. The regulations governing the GISA were amended in December 2018. A company with innovative or creative ideas with potential for development is qualified to apply for GISA registration with TPEx. After TPEx approves the application, the company will start receiving counselling services from TPEx regarding accounting, internal control, marketing and legal affairs. After the counselling period, there is another TPEx review to examine, among other things, the company's management teams, the role of board of directors, accounting and internal control systems, and the reasonableness and feasibility of the plan for capital raising, and, if the TPEx deems it appropriate, the company may raise capital on the GISA. The amount raised by the company through the GISA may not exceed NT$30 million unless otherwise approved. In addition, an investor’s annual maximum amount of investment through the GISA should not exceed NT$150,000, except for angel investors defined by TPEx or wealthy individuals with assets exceeding an amount set by TPEx and having professional knowledge regarding financial products or trading experience.

**Equity-based crowdfunding on the platforms of securities firms**

A securities firm may also establish a crowdfunding platform and conduct equity crowdfunding business. Currently, a company with paid-in capital of less than NT$50 million may enter into a contract with a qualified securities firm to raise funds through the crowdfunding platform maintained by such securities firm, provided that the total amount of funds raised by such company through all securities firms’ crowdfunding platforms may not exceed NT$30 million in a year. The amount of investment made by an investor on a securities firm’s platform may not exceed NT$50,000 for each subscription, and may not exceed NT$100,000 in aggregate in a year, except for angel investors as defined in the relevant regulations.
iv Peer-to-peer lending

While, to date, there are no laws or regulations specifically regulating or governing peer-to-peer lending, the Bankers Association of the Republic of China (the Bankers Association) has promulgated a Self-Disciplinary Rules of Business Cooperation between Member Banks of Bankers Association and Peer-to-Peer Lending Operators (the P2P Self-Disciplinary Rules), and such P2P Self-Disciplinary Rules have been filed with the FSC for record.

According to the P2P Self-Disciplinary Rules, banks may work together with the peer-to-peer lending operators on the following businesses:

- a bank providing a fund custodian service;
- a bank providing a cash flow service;
- a bank providing credit review and rating services;
- a bank extending a facility to the customer (i.e., the P2B model);
- advertising and marketing activities; and
- a bank providing a credit document custody service.

v Loans trading

The general principle under Taiwan’s Civil Code is that any receivable is assignable unless:

- the nature of the receivable does not permit such transfer;
- the parties to the loan have agreed that the receivable shall not be transferred; or
- the receivable, in nature, is not legally attachable.

Receivables under loans, subject to (b) above, are generally transferable; however, a bank is subject to stricter rules that, in general, loans that continue to perform cannot be transferred by a bank except for limited exceptions (such as for the purpose of securitisation). For this reason, Taiwan does not currently have an active secondary loan market.

vi Payment services

Traditionally, payments by wire transfer can only be made through a licensed bank. Payments via cheques and credit cards are also run through banks. Non-banks engaging in credit card-related business and issuance of electronic stored-value cards should also obtain approval from the FSC. In 2015, the Act Governing Electronic Payment Institutions (the E-Payment Act) was enacted. This E-Payment Act regulates the activities of an electronic payment institution, acting in the capacity of an intermediary between payers and recipients to engage, principally, in:

- collecting and making payments for real transactions as an agent;
- accepting deposits of funds as stored value funds; and
- transferring funds between e-payment accounts.

According to the E-Payment Act, an electronic payment institution should obtain approval from the FSC unless it engages only in (a) above and the total balance of funds collected and paid and kept by it as an agent does not exceed the specific amount set by the FSC.
V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

There were no legal or regulatory rules or guidelines in relation to blockchain technology in Taiwan. However, with the rise of certain applications of blockchain technology such as virtual currencies or cryptocurrencies, Taiwan’s regulators have issued several press releases to announce their positions and attitude towards such developments, as well as to educate and warn the general public in Taiwan. Further, the FSC promulgated certain regulations on cryptocurrencies with the nature of securities, which will be described in details below.

On 30 December 2013, both the Central Bank and the FSC first expressed the government’s position toward Bitcoin by issuing a joint press release (the 2013 Release). According to the 2013 Release, the two authorities held that Bitcoin should not be considered a currency, but a highly speculative digital virtual commodity. In another FSC press release in 2014 (the 2014 Release), the FSC ordered that local banks must not accept Bitcoin or provide any other services related to Bitcoin (such as exchange Bitcoin for fiat currency). Such government positions were reiterated by the FSC in an FSC press release on 19 December 2017 (the 2017 Release).

Given the above, in light of the authorities’ attitude, Bitcoin is not considered to be legal tender, currency or a generally accepted medium of exchange under the current regulatory regime in Taiwan; instead, Bitcoin is deemed a digital virtual commodity. The government’s attitude stated in the abovementioned press releases only cover Bitcoin, instead of any other types of virtual currencies or cryptocurrencies (except for initial coin offerings (ICOs) as further explained below). However, we tend to think that any other virtual currencies or cryptocurrencies, if having the same nature and characteristics as Bitcoin, should also be considered as digital virtual commodities.

i ICOs and token offerings; STOs

In response to the rising amount of ICOs and other investment activities regarding virtual currencies or cryptocurrencies, the FSC also expressed the following view on ICOs through the 2017 Release as mentioned above:

a An ICO refers to the issue and sale of virtual commodities (such as digital interests, digital assets, or digital virtual currencies) to investors. The classification of an ICO should be determined on a case-by-case basis. For example, if an ICO involves offer and issue of securities, it should be subject to Taiwan’s SEA. The issue of whether tokens in an ICO would be deemed securities under the SEA would depend on the facts of each individual case.

b If any misrepresentations with respect to technologies or their outcomes or promises of unreasonably high returns are used by the issuer of virtual currencies or an ICO to attract investors, the issuer would be deemed as committing fraud or illegal fundraising.

Given the above, in an ICO (or other types of token offering, such as private token pre-sale before the ICO stage), the core issue in this regard is whether an ICO would be considered as issuing securities under Taiwan’s securities regulations. Under current Taiwan law, the offer and sale of securities in Taiwan, whether through public offering or private placement, are regulated activities and shall be governed in accordance with the SEA, its related regulations as well as relevant rulings issued from time to time by the FSC.
On 3 July 2019, the FSC, by issuing a ruling, officially designated cryptocurrencies with the nature of securities (i.e., security tokens) under the SEA (the 2019 Ruling). According to the 2019 Ruling, security tokens refer to those that:

a. utilise cryptography, distributed ledger technology or other similar technologies to represent their value that can be stored, exchanged or transferred through digital mechanism;

b. are transferable; and

c. encompass the following attributes of an investment:
   • funding provided by investors;
   • funding provided for a common enterprise or project;
   • investors expecting to receive profits; and
   • profits generated primarily on the efforts of the issuer or third parties.

In addition to the 2019 Ruling, the FSC issued a press release on 27 June 2019 to illustrate the key points of the FSC’s policy on security token offerings (STOs). Since then, the FSC and the TPEx have set out the regulation governing STOs (the STO Rules), and the STO Rules were finalised in January 2020. Specifically, the FSC differentiates the regulation of STOs with the threshold of NT$30 million. For an STO of NT$30 million or less, the STO may be conducted in compliance with the STO Rules; an STO above NT$30 million must first apply to be tested in the ‘financial regulatory sandbox’ pursuant to the Sandbox Act and, in case the experiment has a positive outcome, should be conducted pursuant to the SEA. Please see the summary below of certain other major provisions of the STO Rules (i.e., for STOs of NT$30 million or less).

**Regulations on issuance (primary market)**

**Qualifications of the issuer**

The issuer must be a company limited by shares incorporated under the laws of Taiwan and not a company listed on the Taiwan Stock Exchange or TPEx or traded on the Emerging Stock Market. This indicates that a foreign entity may not act as an issuer of an STO programme.

**Types of security tokens that can be issued**

The issuer can only issue profit-sharing or debt tokens without shareholder’s rights, meaning that shares – which is a type of securities under SEA, with regular shareholder’s rights of an issuer, cannot be issued in the form of security token while bonds can be issued as debt tokens.

**Eligible investors and amount limits**

Only ‘professional investors’ are eligible for STOs; where the professional investor is a natural person, the maximum subscription amount is NT$300,000 per STO.

**Issuance process**

Issuers must conduct STOs on a single platform, and the platform operator has the obligation to ensure that the issuer meets the relevant qualifications and that the prospectus be well prepared. Where the platform operator itself is an STO issuer, such issuer should not launch an STO without a prior review by TPEx.
Regulations on trading (secondary market)

Trading mechanism of security tokens

The platform operator should obtain a securities dealer licence and handle the trading by way of price negotiation. The platform operator should be the counterparty to every transaction and should offer a reasonable reference quotation based on the market conditions. In addition, each security token under an STO programme may be traded only on a single platform.

Maximum transaction amount

Where the professional investor is a natural person, the maximum amount of holding under an STO programme is NT$300,000. In addition, the maximum daily transaction limit for each STO is 50 per cent of the total issuance amount under such STO programme.

STO platform operator

Qualifications of the platform operator

The platform operator should obtain a securities dealer licence, have minimum paid-in capital of NT$100 million and provide an operation bond in the amount of NT$10 million.

Total offering amount capacity

The total offering amount of all STOs on a single platform should not exceed NT$100 million. A platform can accept to process a second STO only one year after the security tokens of the first STO have been traded on the platform.

Transfer and record keeping

The platform operator should enter into an agreement with the Taiwan Depository and Clearing Corporation (TDCC) and transmit the trading information such as balance changes and a balance statement to the TDCC to be recorded on a daily basis. The TDCC should provide STO balance inquiry service to investors.

Subscription and trading

Subscription and trading of security tokens should be conducted on a real-name basis and the transactions must be conducted in New Taiwan Dollars under the same name as that featuring on the bank account.

Anti-money laundering

It was reported that, according to Mr Koo, the FSC will regulate the anti-money laundering activities of cryptocurrency trading platforms or exchanges under Taiwan Anti-money Laundering Act after the Executive Yuan (EY) officially authorises the FSC as the regulator of anti-money laundering activities of cryptocurrency trading platforms or exchanges. As at the time of writing, the EY has not granted such authorisation to the FSC so far. In addition, it is unclear at this stage what requirements will be imposed by the FSC on anti-money laundering activities of cryptocurrency trading platforms or exchanges.
VI OTHER NEW BUSINESS MODELS

The legal implications of any new business model should be examined on a case-by-case basis. Unless otherwise provided by law, the legal effect of an action should not be different simply because a new technology is applied. For example, while no specific rules exist that are applicable to the use of a new technology, such as artificial intelligence or automated technology, when offering financial services (except for the ‘automated digital advisory’ as discussed above), a financial institution (such as a bank) may still be subject to relevant outsourcing regulations if the use of a technology could be considered banks outsourcing their operations.

For example, consider self-executing contracts (i.e., smart contracts based on blockchain technology). As a general rule, in Taiwan contracts can be formed by a meeting of the minds, and they can be expressed and proven by way of electronic records, including smart contracts, unless otherwise provided by law. An example of an instance in which a smart contract may not be enforceable is the transfer of real estate, since this requires registration with the regulator and thus may not be completely implemented solely with a smart contract.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

The issue here would be whether fintech business models and related software can be protected by intellectual property rights such as copyright or patent.

i Copyright

Under Taiwan’s Copyright Act, there are no registration or filing requirements for a copyright to be protected by law. However, there are certain features that qualify for a copyright, such as originality and expression. Therefore, while there is a type of copyright called ‘computer program copyright’ under Taiwan’s Copyright Act, whether a work is copyrightable would still depend on whether the subject work has the required components (such as the features described above), especially the feature ‘expression’ (instead of simply an ‘abstract idea’). As to a new copyright developed by an employee of a company during the course of employment, where a work is completed by an employee within the scope of employment, the employee is the author of the work while the economic rights to such work will be enjoyed by the employer unless otherwise agreed by the parties. As to a new copyright developed by a contractor, the contractor who actually makes the work is the author of the work unless otherwise agreed by the parties; the enjoyment of the economic rights arising from the work should be agreed by the parties, or such rights should be enjoyed by the contractor in the absence of such agreement. However, the commissioning party may use the work.

ii Patent

As to patent, an inventor may file an application with Taiwan’s Intellectual Property Office, and the patent right will be obtained once the application is approved. According to the Patent Act of Taiwan, the subject of a patent right is ‘invention’ and an invention means the creation of technical ideas, utilising the laws of nature. As a general rule, business methods are regarded as using social or business rules rather than laws of nature, and therefore may not be the subject of a patent right. As for a fintech-related software invention, if it coordinates the software and hardware to process the information, and there is a technical effect in its operation, it might become patentable. For instance, a ‘method of conducting foreign exchange
transaction’ would be deemed as a business method and thus not patentable; however, a ‘method of using financial information system to process foreign exchange transactions’ may be patentable. As to a new patent developed by an employee of a company during the course of employment, the right of an invention made by an employee during the course of performing his or her duties under employment will be vested in his or her employer and the employer should pay the employee reasonable remuneration unless otherwise agreed by the parties. As to a new invention developed by a contractor, the agreement between the parties should prevail, or such rights should be vested in the inventor or developer in the absence of such agreement. However, if there is a fund provider, the funder may use such invention.

iii Data protection

In Taiwan, personal information is protected by Taiwan's PDPA; the collection, processing and use of any personal data are generally subject to notice and consent requirements under the PDPA. Pursuant to the PDPA, personal data is defined broadly as: the name, date of birth, ID Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities and other information that may directly or indirectly identify an individual.

Under the PDPA, unless otherwise specified under law, a company is generally required to give notice to (notice requirement) and obtain consent from (consent requirement) an individual before collecting, processing or using any of said individual's personal information, subject to certain exemptions. To satisfy the notice requirement, certain matters must be communicated to the individual, such as the purposes for which his or her data is collected, the type of the personal data and the term, area and persons authorised to use the data.

Given the above, if a fintech company wishes to collect, process or use any personal data, it will be subject to the obligations under the PDPA as advised above.

VIII YEAR IN REVIEW

i Digital-only banks

In 2018, the FSC promulgated regulations governing applications for establishing digital-only banks (i.e., banks without physical branches). Three applications were filed with the FSC by 15 February 2019 and all were approved on 30 July 2019. They are expected to start operating in 2020. The establishment of digital-only banks is expected to promote the cooperation of players in different industries and stimulate the application of fintech in everyday life by building up a fintech ecosphere.

ii STOs

In mid-2019, thanks to the prosperous activities of ICOs and the disputes and potential issues regarding illegal fundraising and even fraud, the FSC announced that it would regulate the offering of tokens with the nature of securities under SEA by way of hierarchy management. Soon after the announcement, in January 2020, the FSC and TPEx collaborated and built up the legal regime of STOs by promulgating the STO Rules, exempting STOs of NT$30 million or less from the filing obligation under the SEA and setting up the unique issuing method of STOs. Although it is generally reported that the NT$30 million limit is below the anticipation of STO market players and will have little impact on the securities market, this
regulatory development still represents a big step for the government and demonstrates that it is embracing new technology and making efforts to create an environment that is more fintech friendly.

IX OUTLOOK AND CONCLUSIONS

In July 2019, the FSC announced a proposed amendment to the E-Payment Act. The amendment intends to merge the E-Payment Act and Act Governing Issuance of Electronic Stored Value Cards (E-Card Act), consolidating the legal regime of different kinds of electronic payment methods and expanding the scope of the business of electronic payment institutions. Under the proposed amended E-Payment Act, an electronic payment institution will be opened to provide limited remittance services, which is currently a business exclusive to banks, and other ancillary payment flow services. With the expansion of services that electronic payment institutions can provide, it is anticipated that this amendment will greatly promote the development of the electronic payment ecosphere in Taiwan. The amendment of the E-Payment Act is expected to be discussed in the Legislative Yuan of Taiwan and passed in 2020.
I  OVERVIEW

The general policy and regulatory approach in the fintech ecosystem is to ensure the establishment of a regulatory infrastructure to implement financial and information security. The essential legal and regulatory matters concerning fintech are those regarding payment services, electronic-money institutions (EMIs) and alternative funding methods. This is primarily the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, which regulates the activities and licensing of the payment systems, EMIs and payment institutions in Turkey. The Amendment to the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions (the Amendment), drafted in accordance with the requirements of the Payment Services Directive II (PSSD II) (Directive 2015/2366) stipulates a provision regarding the establishment of the Turkey Payment Services and Electronic Money Association (the Association). It is anticipated that the establishment of the Association shall have a positive impact in the development of the fintech industry. Additionally, the 11th Development Plan of Turkey, published in the Official Gazette on 23 July 2019, includes objectives directly related to Turkish financial technologies ecosystem. The government’s road map which is planned to be created accordingly, will be shaping the current Turkish fintech ecosystem and create a more secure fintech ecosystem in line with international best practices. Turkey has also recently adopted legislation regarding alternative funding methods, mainly different types of crowdfunding.

As for digital information sources regarding fintech, the Turkish Financial Crimes Investigation Board (MASAK), provides guidance and education on the matter. MASAK has also issued Sectoral Guidance Notes addressing financial institutions and banks; however, these do not yet specifically address fintech companies.

Both the government and regulators provide support to financial innovation, but this support is not specifically directed to the financial industry in most circumstances. This support is provided to entities that meet specific criteria. For instance, the incorporation of an entity within a special economic zone (i.e., tech development zone) with its primary business activity listed as technology would qualify the said entity for tax benefits. The Technology Development Law governs this field and provides for lower corporate income tax, withholding tax, income tax exemptions, employer social security contribution support payments and value added tax exemptions.

1 Cigdem Ayozger Ongun is a managing partner, Filiz Piyal is a managing senior associate and Deniz Erkan is an associate at SRP-Legal.
A developing and vibrant fintech climate exists in Turkey, the regulatory approach may be described as fintech-friendly, although cryptoassets are yet to be defined under Turkish legislation. The market is open for new investments. Electronic payment institutions and EMIs have emerged as new sectors in financial intermediation. As of February 2020, there are 34 licensed payment institutions and 18 EMIs. Technological innovation, accelerating the increase in the number of electronic and mobile payments providers and the emergence of new types of payment services in the fintech market have resulted in regulatory changes. The Amendment, which entered into force on 1 January 2020, contributes to the development of an innovation climate in the fintech ecosystem as it introduces new types of payment services.

II REGULATION

i Licensing and marketing

Turkey regulates a comprehensive scope of financial services and activities. Financial institutions are obliged to obtain authorisation from relevant regulators (i.e., the Banking Regulation and Supervision Agency (BRSA), the Capital Markets Board (CMB) and the Treasury) to be incorporated and conduct financial activities. Licensing requirements apply in all cases that involve the provision of payment and e-money services. The market is highly regulated and there are significant financial barriers of entry into the market. Payment services and e-money services can solely be offered if the provider is a licensed entity. This being said, a licensed entity can be incorporated to offer payment services only if it is incorporated as: a financial institution that falls under the definition of a bank as listed within Turkey’s banking legislation (namely the Banking Law), an EMI or a payment services provider.

According to the Amendment, the Central Bank of the Republic of Turkey (CBRT) is the authorised body to supervise and regulate e-money and payment service providers instead of BRSA. In addition to the CBRT, MASAK also regulates fintech products and services in terms of money laundering proceedings for crime and terrorist financing.

Sale and marketing of financial services and products may fall under the supervision of the CMB or the BRSA. The CMB’s Communiqué on Principles on Investment Services and Activities and Ancillary Services No. III-37.1 (the Investment Services Communiqué) and the BRSA’s Regulation on Bank’s Procurement of Support Services impose certain restrictions on financial service providers as well as the vendors providing the sales and marketing of financial services in Turkey.

Pursuant to Article 12 of the Investment Services Communiqué, intending advertisement and marketing activities directly or through persons or institutions residing in Turkey with respect to investment services provided by the institutions residing abroad, shall be deemed to be intended for the persons residing in Turkey, and shall also be subject to restrictions.

Automated digital advice is not specifically regulated under the Turkish legislation; however, if the advisory service to be carried is in relation to a regulated financial activity, regardless of its form – either digital or in person – it may be subject to an authorisation or an exemption.

The Regulation on Establishment and Activities of Asset Management Companies, Article 6, sets forth that asset management companies must obtain authorisation from the CMB prior to their establishment in order to carry out their activities.

Providing credit references or credit information services in Turkey is a regulated activity under the Banking Law. A Risk Centre is established within the Banks Association
of Turkey for the purpose of collecting the risk data and information of clients of credit institutions and other financial institutions to be deemed eligible by the Banking Regulatory and Supervisory Board, and ensuring that such information is shared with said institutions or with the relevant persons or entities themselves or with real persons and private law legal entities if approved.

Kredi Kayıt Bürosu (KKB) founded under Article 73/4 of the Banking Law conducts all operational and technical activities through its own organisation as an agency of the Risk Center of the Banks Association of Turkey and provides data collection and sharing services to 180 financial institutions that are members of the Risk Centre.

ii Cross-border issues

Under Turkish law, a licence to provide financial services in Turkey cannot be obtained unless the company is governed by the Turkish law. Turkey is not a member of the EU (though a candidate in the negotiations for full membership) or the European Economic Area, nor a party to an agreement for passporting financial services across Europe. Therefore, a Turkish financial institution cannot passport its authorisation into the European Economic Area Member States or any other jurisdiction, and reciprocally foreign financial institutions cannot operate without required licences in Turkey.

The Communiqué on Foreign Capital Market Instruments, Depository Receipts and Foreign Investment Fund Shares published by the Turkish Capital Market Authority No. VII.128.4 includes certain requirements that must be fulfilled by the issuer. Some of these can be included as regulated activities that may be passported into the Turkish jurisdiction. However, a general application of passporting of regulated activities into the Turkish jurisdiction is not possible.

A fintech company is required to be incorporated and licensed in the local Turkish jurisdiction. Apart from being licensed by the Banking Regulation and Supervisory Authority, it must be incorporated as a corporation, with minimum capital requirements, and there are limitations on controlling ownership of shares and share transfers. Said requirement also applies to companies that provide cross-border services and products, and whether the products are actively marketed or the client in the jurisdiction solicits the service or product is not relevant.

Pursuant to the Direct Foreign Investment Law and the Banking Law, there are no restrictions or limitations on ownership of companies by foreigners. On the contrary, direct foreign investments are promoted by the former.

III DIGITAL IDENTITY AND ONBOARDING

There is no official national digital identity in Turkey for the time being as type of a foundational identification system. There is no specific regulation regarding digital identity in the Turkish legislation. However, there are separate pieces of legislation concerning electronic capture and storage attributes or credentials that may uniquely identify a person and create a digital identity. The Electronic Signature Law lays out the principles regarding digital identification. Following the Electronic Signature Law, the Communiqué on Electronic Signature and Relevant Procedures and Technical Criteria (the Electronic Signature Communiqué) has also set a technical basis regarding the electronic signature that may be used in the creation of a digital identity.
As per the Electronic Signature Law, electronic signatures may be issued by electronic certificate service providers, which may be established as public or private entities.

The scope of the use of digital identity has not been regulated; however, it is anticipated by the Information and Communication Technologies Authority that electronic signatures will be used for all kind of applications (e.g., placement exams and passports), inter-institution communication (police departments, General Directorate of Civil Registration and Nationality), social security applications, health applications (health personnel, hospitals and pharmacies), tax payments, electronic voting systems, online banking, insurance transactions, e-agreements and online orders. In addition, there are several examples of functional identification systems supplied by mobile network providers and digital operators provide blockchain service for identity management.

There are a couple of regulatory challenges as to the implementation of fully digitalised onboarding of clients. Laws in Turkey require a written signature to accept someone as a bank customer. In addition, know your customer (KYC) requirements stipulate the application of customer identification on a face-to-face basis. Although there are some regulatory draft proposals that may pave the way for digital onboarding of financial customers in the future, it is not legally permissible to use video technologies for the implementation of KYC either. Therefore, these regulatory requirements are making it hard to design a seamless digital onboarding process for financial service providers to carry out fully digitalised onboarding.

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

There is no specific regulation governing cryptoassets, and the debate regarding the legal definition of cryptoassets continues. The Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions and its supplemental secondary legislation regulates the market and the concepts such as e-money, digital wallets, and digital currencies. Due to a lack of agreement among regulatory and supervisory authorities, the status of cryptoassets is yet to be defined under Turkish law. If cryptoassets are considered a security, the Law on Capital Markets shall be the governing legislation; however, if cryptoassets are defined in a way similar to e-money, then Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions shall be the governing legislation.

The general rules and principles regarding investment funds are mainly regulated under Law on Capital Markets. The Capital Markets Board (CMB) regulated further details regarding the establishment and activities of investment funds under the Communiqué on the Principles of Investment Funds (III.52.1) (the Investment Funds Communiqué) and also introduced the Investment Funds Guide (the Guide) with Resolution No. 19/614, in order to clarify the rules and principles stipulated in the Communiqué. The Communiqué Amending the Investment Funds Communiqué (the Amending Communiqué) entered into force upon its publication in the Official Gazette on 12 March 2019, and the Guide was also amended on the same date to reflect the changes introduced through the Amending Communiqué.

The legislation governing the scheme of crowdfunding is newly emerging in Turkey. The Communiqué on Equity Based Crowdfunding (the Crowdfunding Communiqué) was published in the Official Gazette on 3 October 2019 and designates the CMB of Turkey as the supervisory regulatory authority. Providing alternative finance products, services, and collective investment methods fall under the scope of the Crowdfunding Communiqué. In addition to that, credit lines and loans are not listed as permissible services to be offered by
payment service providers and EMIs since the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions sets strict prohibitions on the permissibility of offering credit lines or loans by payment service providers or EMIs.

The Banking Law Amendment, which was published in the Official Gazette on 25 February 2020 and became effective on the same day, introduced the concept of crowd-lending by the inclusion made to the Capital Markets Law. Accordingly, the CMB is empowered to make a determination regarding crowdfunding activities by collecting money from the public based on partnership or borrowing. However, since the secondary legislation regarding crowd-lending has not yet been drafted, there are no specific regulations regarding requirements, restrictions and licensing issues. Additionally, peer-to-peer lending is not currently regulated in a manner synonymous with the definition found under PSD II.

As per the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, payment services and e-money services can solely be offered if the provider is a licensed entity and has been incorporated as a financial institution, an EMI or a payment services provider.

There are significant duties levied upon financial institutions regarding the duty of confidentiality within the Turkish legislation, namely the Banking Law, the Turkish Commercial Code, the Turkish Criminal Code and the Personal Data Protection Law. This duty limits the sharing of data in a manner that would be considered as promoting competition. However, according to the Regulation Detailing the Principles and Procedures on Accounting Practices and Document Retention and the Communiqué on Financial Charts and Explanations and Footnotes to be Made Public, banks and financial institutions must make banking data available to the BRSA. Article 9 of the Amendment to the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, stipulates that the CBRT is empowered to enact secondary legislation that may require payment service providers to share data with other payment service providers.

The Amendment extends the list of payment services by introducing the definitions of ‘payment initiation services’ and ‘account information services’. However, the banks would not be legally required to offer third-party providers access to their customers’ accounts via open application programming interfaces (APIs), as long as the CBRT does not issue a secondary legislation on data sharing practices. Nevertheless, some Turkish banks have already released their APIs to promote third-party developers.

V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

There is no specific regulation governing cryptocurrencies, but there are no specific provisions under Turkish legislation that prohibit individuals from owning and exchanging cryptocurrencies. Turkish legislators have not identified a category for cryptocurrencies or tokens and not yet enacted any special rules for the legal treatment of cryptocurrencies. Despite the fact that there is no legislation governing cryptocurrencies, there exist several cryptocurrency exchange platforms operating in the Turkish fintech ecosystem.

There is no specific regulation governing initial coin offerings (ICO) or token generation events either. However, as mentioned above, if in the future cryptoassets are classified as securities, the Law on Capital Markets shall be the governing legislation, and thus the criteria stipulated under this law shall apply. However, the CMB has not yet classified or assessed security tokens.
Since tokens are not classified or regulated under the Turkish legislation, tokens may not be linked to underlying assets, and shares and bonds may not be issued in the form of a token.

Turkish anti-money laundering legislation, namely the Law on Preventing Laundered Criminal Income and its supplemental regulations, requires that fintech companies (dealing with cryptocurrency and tokens) implement procedures to combat bribery. The appointment of a compliance officer, identity verification of account holders, together with reporting of suspicious transactions are commonplace requirements the regulation imposes upon fintech companies. MASAK also regulates fintech products and services in terms of money laundering proceedings for crime and terrorist financing.

Since cryptocurrencies and tokens are not regulated in Turkish legislation, it is not possible to impose tax on such exchanges. In order to be able to impose tax on cryptocurrencies and tokens, first they must be defined under legislation and the tax law must be amended to include them. If cryptocurrencies were to qualify as commodities in Turkey, the income derived from the exchange of said cryptocurrencies would be subject to income tax. However, for the time being, gains derived from cryptocurrencies are not included within the types of income subject to income tax.

There is no regulation allowing or restricting the offering of tokens to residents from abroad.

VI OTHER NEW BUSINESS MODELS

Pursuant to the Law of Obligations, for a contract to be legally binding, there has to be an offer and an acceptance, and the parties should intend said contract to be legally binding. Given the nature of self-executing contracts, without separate legislation to regulate them, their enforceability may be challenged on the grounds that they restrict parties' negotiation power over the terms and conditions of an agreement. In addition, self-executing contracts are not legally enforceable for formal contracts specified by certain laws (e.g., real estate contracts and vehicle sales agreements).

There is no regulation regarding artificial intelligence (AI) under Turkish legislation; however, the Digital Transformation Office, structured under the Presidency, has been assigned the task of leading the AI transformation process.

Product price comparison websites are not specifically regulated under Turkish legislation and general law principles shall apply.

Equity-based crowdfunding has been introduced as a new business model as per the Communiqué on Equity Based Crowdfunding (the Crowdfunding Communiqué), which was published in the Official Gazette on 3 October 2019, the scope of the Crowdfunding Communiqué includes providing alternative finance products, services and collective investment methods. The Crowdfunding Communiqué regulates equity-based and share-based crowdfunding, and fundraising from the public through equity-based crowdfunding. As per the Banking Law Amendment, the initial steps for the regulation of lending-based crowdfunding have also been taken.

The Amendment to the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions broadened the scope of the list of payment services by introducing the definitions of ‘payment initiation services’ and ‘account information
services’. This paved the way for financial institutions to offer third-party providers access to their customers’ accounts via open APIs. Some Turkish banks have already released their APIs to promote third-party developers.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Turkey does not afford patent protection to software-implemented inventions and business methods. Copyright protection is the method that can be utilised for protecting ownership rights over software. Copyright protection is a natural protection offered to the creator starting from the moment the property is offered or made available to the public. There is no application similar to that of a patent application that is required of a copyright holder.

A patent establishes protection over the invention and grants property rights over it. After submission to the local patent office, a patent will be assessed and upon successful display of the patent holder’s claims of novelty and function, a patent right will be granted. However, business methods and software-implemented inventions cannot be comprised under patent protection.

There are two distinct regulations regarding the duty of confidentiality. The first piece of legislation, which governs confidentiality of banking and financial information, is the Banking Law. The second is the Personal Data Protection Law, which prohibits or sets limitations on the disclosure, processing and transfer of personal information (that would also include client information).

Additionally, payment service providers and EMIs are subject to the duty to transfer financial data to the BRSA regarding what the Banking Law defines as ‘banking data’. The Amendment to the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, states that the CBRT holds the right to enact secondary legislation that may require payment service providers to share data with other payment service providers.

However, pursuant to the Banking Law Amendment published on 25 February 2020, save for the mandatory provisions of the relevant legislation, client information has been specified as a client secret and the criteria regarding processing and transfer of said information shall be realised in accordance with the Personal Data Protection Law. Even in cases where the client grants explicit consent regarding the processing of his or her personal data, this data may not be transferred or shared domestically or abroad without the explicit request or order of the client.

VIII YEAR IN REVIEW

One of the most important developments affecting the fintech industry in the last 18 months was the decision of the Competition Board to revoke the exemption rights granted to the Interbank Card Center (ICC) and the activities it performed under the ICC Express brand, where it acted as a payment service provider, a digital wallet and a payments data house. Since the original licence granted to ICC Express was regarding permission to act as a clearinghouse for exchanges and authorisation transactions, when ICC Express started to provide other services outside this scope its licence was revoked upon the decision of the Competition Board dated 30 May 2019. The revocation of this licence, not effective until mid-2020, presents a risk as to how antitrust provisions may be applied to fintech companies that participate in their designated markets via an exchange.
The Amendment to the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, which authorises the CBRT instead of the BRSA to supervise and regulate e-money and payment service providers, is also of an important nature. The said Amendment is also relevant to the development of the fintech industry as it introduces new types of payment services namely account information services and payment initiation services.

The introduction of equity-based crowdfunding as per the Crowdfunding Communiqué, which provides alternative finance products, services and collective investment methods; and the initial steps regarding lending-based crowdfunding being taken pursuant to the Law on the Banking Law Amendment are other developments worth mentioning.

One of the most important indicators of the health of the fintech ecosystem of Turkey in 2019 was the number of start-ups that made successful exits. Eight fintech start-ups exited successfully in 2019, which shows that foreign investors have renewed their interest in Turkey and this has created momentum in the industry.

IX OUTLOOK AND CONCLUSIONS

Despite the absence of an applicable legal framework, a vibrant fintech industry is developing in Turkey. Fintech is transforming finance, business and transaction models, and challenging the regulations constantly. Turkish regulatory bodies are closely monitoring the developments and preparing regulations to react to and meet the requirements generated by the technological developments.

From a regulatory perspective, there is no specific definition of cryptoassets and no restrictions on engaging in cryptocurrency transactions in Turkey. There have been developments in the legal and regulatory landscape for equity-based crowdfunding, lending-based crowdfunding, open banking and the protection of client information. New regulations are being adopted that enable the entry of new actors into the fintech market, increase cooperation with the banking sector and facilitate the development of fintech in Turkey. These include the recent Amendment to the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, which reorganises the regulatory framework for payment and electronic money services and introduces new definitions of account information services and payment initiation services in line with the PSD II.
I

OVERVIEW

The UK is one of the world’s leading centres for ‘technology applied to financial services’ (the Department for International Trade’s definition of fintech),\textsuperscript{2} and the market has continued to grow year on year. It benefits from the UK’s financial services regulatory regime, which is well established, and the supervision of that regime by the Financial Conduct Authority (FCA), which maintains a reputation as one of the gold standard regulatory bodies worldwide. The trend in the UK over the past decade has been towards ever increasing regulation, and the current climate is no exception. In the past year, legislation has been brought forward to effect the onshoring of EU laws once the current Brexit ‘implementation period’ ends on 31 December 2020. The FCA has also clarified the rules governing cryptoassets.

There are no dedicated fintech tax incentives in the UK, but there are various features of the UK tax regime that make it attractive for fintech businesses. There are incentives for companies, for example, R&D incentives for both capital and revenue expenditure and the ‘patent box’ regime.\textsuperscript{3,4} Additionally, there are incentives for investors and management, including seed enterprise investment schemes, enterprise investment schemes, venture capital trust reliefs, entrepreneurs’ relief, investors’ relief and tax-advantaged share option arrangements.

The UK, like many other jurisdictions, is still addressing some of the transfer pricing and taxable presence problems arising out of fintech businesses. These depend on the value that is placed on a decentralised system, and new types of questions are likely to need to be answered as to what is required for a taxable presence in a country. The starting point for UK tax is to check whether there is a permanent establishment, and typically this will

\textsuperscript{1} Gareth Malna is an associate and Sarah Kenshall is a director at Burges Salmon LLP.


\textsuperscript{3} The ‘patent box’ is simply a calculation, though the way in which the patent is owned and used within a group structure can make the calculation and attribution of relevant amounts easier administratively. It allows the company to benefit for a low tax rate of 10 per cent for profits within the ‘box’. The benefit of the regime is no longer available for acquired patents; however, it does cover cases where part of the relevant work was subcontracted. For fintech companies, patents that qualify have become more common. Nevertheless, it is critical to note that because the regime only applies to profits related to patents registered with the UK Intellectual Property Office or the European Patent Office or an European Economic Area State, the benefit of the more flexible regime for software patents in certain jurisdictions (for example, the US and Singapore) is not available.

\textsuperscript{4} There is no equivalent regime for other forms of intellectual property such as copyrights and trademarks.
involve a physical presence. However, there are also anti-avoidance provisions designed to prevent an avoided permanent establishment or profit fragmentation, and in some cases the arrangements around a fintech business will need to be reviewed to see if there is a risk of triggering these provisions. In some cases, it will be harder to judge how these might apply to a global supply chain compared with a more traditional business.

II REGULATION

i Licensing and marketing

Licensing

The FCA is technology neutral in its considerations on whether a firm is caught by the regulations and, therefore, the source and details of the rules that apply to fintech businesses operating in the UK will depend on the activities being carried on by each business. As a starting point, businesses will have to consider the general prohibition set out in Section 19 of the Financial Services and Markets Act 2000, which provides that it is a crime for any person to carry on regulated activities by way of business in the UK unless that person is authorised or exempt.5

The list of regulated activities caught by the general prohibition is set out in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO) and includes, pertinent, accepting deposits,6 issuing electronic money, effecting and carrying out contracts of insurance,7 advising on or arranging deals in investments,8 dealing in investments as agent or principal, providing credit information services and operating an electronic system in relation to lending.9 These are known as ‘specified activities’, and to be regulated activities must relate to certain specified investments also set out in the RAO. Specified investments include electronic money, contracts of insurance, shares, units in collective investment schemes, rights under a pension scheme and credit agreements.10 It does not matter whether services are offered digitally or in person; an entity carrying on the activities specified in the RAO by way of business in the UK11 will be carrying on a regulated activity for which it must be authorised or exempt.

Where the activities of a business relate to the provision of payment services then the regime implemented in the Payment Services Regulations 2017 (PSR) will apply to the authorisation, registration and conduct of business obligations of those businesses. These aspects are discussed in more detail in Section IV.

Authorisation and registration applications for carrying on regulated activities under FSMA or specified activities under the PSRs must be made to the FCA and, in some cases, to

5 See Sections 19 and 20 FSMA.
6 Relevant for neo-banks acting with full deposit-taking permissions such as Starling and Monzo who were both granted permission during 2018.
7 Relevant for those platforms offering peer-to-peer insurance.
8 Relevant to digital wealth platforms such as Nutmeg and MoneyFarm.
9 Directly applicable to loan-based crowdfunding platforms such as FundingCircle.
10 See Part III of the RAO.
11 The question of whether an activity is being carried on ‘in the United Kingdom’ has to be answered in the context of each activity. Entities that arrange deals in investments are said to be carrying on that activity from the place of their establishment, whereas the activity of advising is said to be carried on where the advice is received.
Once authorised or registered, either or both of the regulators will continue to regulate the activities of the firm. All firms are regulated by the FCA as regards their conduct of business, but larger trading institutions will also be supervised by the PRA, which focuses on financial concerns that have an ability to negatively impact the broader market and economy.

The authorisation process is a lengthy and time-consuming one, and the scope of permissions that firms are required to obtain are not always clear. With that in mind, the FCA launched its regulatory sandbox in June 2016. The sandbox is open to authorised firms, unauthorised firms that require authorisation and technology businesses, and seeks to provide those firms with, among other things, a reduced time-to-market at (potentially) lower cost including by offering a restricted authorisation path, which allows those firms to operate in a limited manner under the close supervision of the FCA. As of May 2019, 29 businesses were accepted into the fifth cohort of the sandbox, including Barclays, British Heart Foundation and Open Banking Implementation Entity. The success of the sandbox grows each year and this year the FCA received an unprecedented 99 applications.

Despite the more informal route that may be open to firms accepted into the sandbox, no special fintech licence or permission regime applies to fintech firms looking to operate in the UK.

**Marketing**

Subject to certain notable exceptions, firms may generally market themselves freely in the UK as long as any advertisements or marketing materials are accurate, legal, decent, truthful, honest and socially responsible.

Firms may not, however, in the course of business communicate an invitation or inducement to engage in investment activity (a financial promotion) unless the firm is authorised or the content of the communication is approved by an authorised person. Breaches of the restriction on financial promotions carry criminal consequences.

The terms ‘invitation’ and ‘inducement’ are typically given their natural meaning and, as such, communications that include a promotional element, (rather than those that seek merely to inform or educate about the mechanics or risks of investment) will be caught by the financial promotion restriction.

A number of exemptions may cause a financial promotion to fall outside of the restriction and, therefore, may freely be made by unauthorised firms within the boundaries of the applicable exemption. Alternatively, unauthorised firms may enter into arrangements under which an authorised entity reviews and approves each promotion at the time it is

---

12 The PRA supervises around 1,500 banks, building societies, credit unions, insurers and major investment firms.

13 The FCA can also offer through the sandbox: (1) the ability to test products and services in a controlled environment; (2) support in identifying appropriate consumer protection safeguards to build into new products and services; (3) better access to finance; and (4) individual guidance, informal steers, waivers and no enforcement action letters. For further details on the sandbox see https://www.fca.org.uk/firms/regulatory-sandbox.

14 i.e., they must not encourage illegal, unsafe or antisocial behaviour.

15 Section 21 FSMA.
made. This is a structure often implemented in crowdfunding, for example, where a business seeking equity investment through the crowdfunding platform is required to get the platform (which will be authorised) to sign off on the promotion before it is listed on the site.

Authorised firms that make financial promotions in compliance with the financial promotion restriction will also need to bear in mind the additional conduct rules for financial promotions set out in Chapter 4 of the Conduct of Business Sourcebook of the FCA Handbook.

ii Cross-border issues

As identified in the previous section, for a regulated activity to be carried on there must be some link between the activity and the UK. As such, where there is a cross-border element to the services or activities it will be necessary, from a regulatory perspective, to consider where the activity is actually carried on. This will inform the analysis of whether the firm carrying on that activity requires authorisation in the UK under the process described above. Where a business does not carry on any regulated activities in the UK then it will be able to provide those services in the UK, either on a cross-border basis or from a branch office set up in the UK.

As regards those fintechs not based in – but that intend to provide regulated activities in – the UK, it is currently necessary to consider separately those that are based in Europe and those that are based in other continents; though that is likely to change after the end of the Brexit implementation period on 31 December 2020 unless the UK and EU successfully negotiate a free trade agreement.

For those that are based in Europe, the complex web of EU passporting regimes continues to apply, depending on the activities carried on by the fintech business. For example, electronic money institutions may passport under the Second Electronic Money Directive, while fintechs that provide insurance intermediary services may use the regime under the Insurance Distribution Directive. The broadest passporting regimes (i.e., those that cover the most activities relevant to fintechs) are set out in the Markets in Financial Instruments Directive (MiFID II) and Payment Services Directive (PSD2). EEA-based firms should not expect current passporting arrangements to continue after the Brexit implementation period ends. This means that they will need to plan for a range of possible scenarios for the end of the Brexit implementation period, including that the activities they conduct might not be covered by future arrangements agreed between the UK and the EU.

Those firms outside the EU looking to provide similar services in the UK will need to seek separate authorisation in the UK in relation to the regulated activities they intend to carry on.

16 2009/110/EC.
17 (EU) 2016/97.
III DIGITAL IDENTITY AND ONBOARDING

There is no official national digital identity in the UK at present. The Government Digital Service has been running GOV.UK Verify as a secure way of accessing government services, but it has largely been considered a failure and it was announced at the end of 2018 that it would be transitioned to the private sector.

Despite that, a number of fintech firms are employing ever more sophisticated digital onboarding services, with the neo-banks in particular now very good at onboarding clients with little more than photographs of passports and a short video. Meanwhile, the market for firms who claim to be able to use cryptographic hashing to create a digital identity for an individual is growing rapidly in the UK. If successful, these services will enable individuals to verify their identity to third parties using only a very small amount of data (e.g., their personal hash, which is a cryptographically generated code combining all elements of that individual’s identifying personal data, with a checksum item forming part of the personal hash calculation, such as the individual’s year of birth. In this case the year of birth acts as a way of validating the personal hash and, therefore, the identity of the individual in question).

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i Digital markets and funding

The UK has a very strong market in crowdfunding, peer-to-peer (P2P) lending and payment services, all of which sit alongside the UK’s world-leading financial services marketplace.

The crowdfunding market in the UK is particularly mature and sophisticated – so much so that in July 2018 the FCA launched a consultation\(^{19}\) into the market in order to identify whether the existing regulatory framework is still relevant and robust enough to ensure good standards of business are practised by the platforms, particularly where retail investors are involved.

Certain crowdfunding activities require authorisation by the FCA and others do not. All crowdfunding platforms are subject to the FCA’s general high-level standards, including the Principles for Businesses and specific Conduct of Business rules, for example in relation to financial promotions. However, there are differences in the detailed regulatory frameworks that apply to investment-based and loan-based (or P2P) crowdfunding platforms.

Investment-based crowdfunding has evolved from more traditional ways of seeking equity-based investments, and the FCA regulates it as such. Therefore, an investment-based platform will usually ask for authorisation from the FCA to carry on activities such as arranging deals in investments (Article 25 RAO), dealing in investments as an agent (Article 21 RAO) and advising on investments (Article 53). Platforms that provide a nominee structure must also apply for a safeguarding and administration of assets permission (Article 40).

Operating a P2P platform was not adequately captured under the existing list of regulated activities, so, in 2014, the FCA introduced the new activity of operating an electronic system in relation to lending (Article 36H RAO), which captures most of what P2P platforms will be carrying on in practice. However, care should be taken if other regulated activities are built into the business model, such as credit broking, debt administration and debt-collecting, each of which require separate permission from the FCA.

\(^{19}\) CP18/20, which closed in October 2018 with a final policy statement due in Q2 2019.
The creation of secondary markets on platforms is not prohibited, but is becoming increasingly unusual with the more established platforms because of the additional regulatory burden of doing so (not least because of the potential financial promotion issues). It is more common for platforms to create venture capital-like fund structures that give investors the ability to exit the fund without having to find other users to buy their units.

**ii Payment services**

The UK is also a world leader in payment services. Firms will often seek authorisation from the FCA even where they do not intend to serve customers in the UK in order to benefit from the halo effect of being a UK-regulated firm when considering international expansion.

Payment service activities regulated under the PSRs in the UK include, among other things, services relating to the operation of payment accounts (e.g., cash deposits and withdrawals from current accounts and savings accounts), execution of payment transactions (whether covered by a credit line or otherwise), card-issuing and money remittance. PSD2, as implemented by the PSRs, also creates authorisation and registration regimes for payment initiation service providers (PISPs) and account information service providers (AISPs), two activities newly defined in 2017 that capture those businesses looking to utilise open banking standards to provide consumers with information about their finances, or that facilitate payments directly from users' bank accounts without the need to use a payment card.

Firms offering payment services are required to identify at the outset whether they will apply for registration or authorisation under the PSRs. Small payment institutions (SPIs), small electronic money institutions (EMIs) and firms that will only offer account information services can apply to be registered as such, or as a registered account information service provider (RAISP), and a lighter touch registration and conduct regime will apply to those firms. Firms that do not qualify as an SPI, small EMI or RAISP but that intend to carry on payment services in the EEA must apply for authorisation and follow more onerous conduct of business requirements. These alternative routes are particularly popular where available.

PSD2 and the PSRs also facilitated new open banking standards, requiring banks and building societies to give third parties access to customers’ accounts and data where the user consents to it. At the moment, only the UK's nine largest banks and building societies must make customer data available through open banking, but a number of smaller banks and building societies have also opted in to the regime. Relevant third parties that benefit from the open banking regime include PISPs and AISPs, who are able to use customer account data to provide these new breeds of services.

Take-up was initially slow, but in 2019 open banking surpassed 1 million users for the first time. With a greater number of consumers and small businesses authorising their bank accounts to be connected with authorised third parties, responsibility for protection of their data rests with a wider ecosystem of providers. This raises challenges around security, the onward supply of data and the combination of data with other datasets.

---

20 Firms operating below an average monthly turnover in payment transactions of €3 million.
21 Firms in which total business activities will not exceed an average of €5 million of outstanding e-money immediately before registration.
22 Open banking is one of a series of regulatory remedies mandated by the UK Competition and Markets Authority requiring nine UK banks to implement a common standard API to allow third parties to access customer bank accounts (with customers' explicit consent)
V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS

Blockchain technology continues to capture the imagination in the UK, and the number of businesses adopting the technology for their own purposes is indicative of longer term trends. To date, key financial industries utilising the technology include the UK insurance and crowdfunding sectors, with asset management following slightly behind.

Of course, blockchain’s original use in cryptoassets continues to be relevant, though that market is under a period of significant flux at the time of writing. This is, in part, due to the global development of rules and regulations that has created a period of instability and regulatory uncertainty. While the UK has not implemented any specific cryptoasset laws or regulations, the FCA has carried out work on cryptoassets, both as part of a broader UK Cryptoasset Taskforce and independently. The output of that work is the publication of Policy Statement 19/22, which is intended to help market participants to understand whether the cryptoassets they use are within the regulatory perimeter. In general, cryptocurrencies are not separately regulated by the FCA provided that they are not part of other regulated products or services. Instead, cryptoassets will fall within one of two categories – regulated tokens and unregulated tokens. The latter category does not require regulation and we have not considered those tokens further for these purposes. Regulated tokens can be further broken down into two categories – security tokens and e-money tokens.

Security tokens are tokens that provide rights and obligations akin to specified investments as set out in the RAO, including those that are financial instruments under MiFID II. Consequently, whether a cryptoasset will be treated as a security token will depend on its characteristics such as (1) any contractual rights and obligations the token-holder has by virtue of holding or owning that cryptoasset, (2) any contractual entitlement to profit-share or (3) whether the token is transferrable and tradeable on exchanges.

Separately, the new category of e-money tokens is based on the definition of e-money under the Electronic Money Regulations 2011 (EMR), that is, electronically stored monetary value as represented by a claim on the issuer that is (1) issued on receipt of funds for the purpose of making payment transactions; (2) accepted by a person other than the electronic money issuer; and (3) not excluded by Regulation 3 of the EMR.

Although it is clear that potential anonymity (or, more precisely, pseudonymity) afforded to individuals by cryptoassets means that they may have a role in money laundering and terrorist financing, the applicability of the existing money laundering regulations in the UK is not straightforward. To address that issue, the FCA has taken over supervision of anti-money laundering for cryptoasset businesses under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), effective from 10 January 2020. The MLRs have been amended to bring cryptoasset exchange providers (including providers of automated teller machines (ATMs), peer-to-peer providers and issuers of new cryptoassets) and custodian wallet providers, within scope of the regulations. Businesses carrying on those activities will need to register with the FCA.

The UK has been reluctant to legislate for the tax treatment of cryptocurrency and crypto-token offerings, and HMRC, the UK tax authority, has focused instead on fitting this within existing tax provisions. However, it was recognised that, in the light of the Final Report from the Cryptoassets Taskforce in October 2018, some clarification was needed, as HMRC’s 2014 guidance focused mainly on certain types of cryptocurrency and was very limited in scope. HMRC therefore produced revised guidance, covering the tax treatment of cryptoassets for individuals and where these are used as a form of employee reward (in
December 2018) and the tax treatment of cryptoassets for companies and businesses (in December 2019). Unfortunately, there has so far been no detailed public clarification of HMRC’s view on the treatment of ICO and initial token offering issues for the issuing entities, but it is hoped additional guidance will become available in the near future.

Cryptoassets may currently be marketed to UK residents from other jurisdictions, but the UK financial promotion regime will apply and market participants will need to ensure that any financial promotion of products and services, whether regulated or unregulated, is carried on in a way that is clear, fair and not misleading. Firms must make clear in their promotions which activities are, and are not, regulated, especially when marketing their FCA-authorised status, so care will need to be taken in this regard.

VI OTHER NEW BUSINESS MODELS

The UK is awash with new business models. Of the new models available, 2019 was the year in which open banking really started to take off, with a rise in the number of AISPs becoming operational. Other popular business models include robo-advisers (including fully automated investment processes), e-wallets, crowdfunding, information aggregators and trust-based platform arrangements. Third-party financial comparison sites are commonplace, with insurance the largest category in both the consumer and business sectors. These sites are subject to the usual credit broking and insurance-related regulation (among others), and the same data protection and competition rules as any other business.

Self-executing, or ‘smart’ contracts are permitted, and the usual legal framework for contracts applies to them. That means there are a few legal questions still unanswered, especially around liability and agency. When it comes to making corrections, the court is the default option, unless an alternative was agreed in the contract.

Finally, use of big data is also on the rise as a tool to aggregate, analyse and increase the value of vast datasets. For example, the UK’s implementation of open banking promises a world of build-your-own services and jealously guarded white-labelling agreements. To facilitate data transfers we are seeing trust-based arrangements with clear accountabilities and risk allocation for all participants, careful governance and security governing access, including third-party supply chain players.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

i Intellectual property

There are no intellectual property protections that are peculiar to fintech. However, in common with all evolving technologies, some fintech technologies do test the limits of the existing legal framework, this having not been written with these new technologies in mind. The most notable challenges come from blockchain technologies and technologies delivering artificial intelligence and machine learning applications.

The most important intellectual property rights for artificial intelligence are confidentiality, copyright and patent rights. The laws of confidence pose no unusual issues
for artificial intelligence. However, from a wider financial services policy perspective, it would be preferable for innovators to disclose AI innovations rather than opt to keep these as trade secrets, so other protections come to the fore.

Copyright raises some issues in respect of ownership of the output of artificial intelligence, but otherwise copyright protection of source code remains as applicable to artificial intelligence software systems as it does for more traditional software systems.

It is in the realms of patent that the interesting issues around protection arise. In the UK, and under the European Patent Convention, in order to be granted a patent, the invention must be new, inventive, and capable of industrial application and not specifically excluded from protection as a patent. Mathematical methods are excluded, as are computer programs, which are, of course, at the heart of artificial intelligence development.

This is not to say artificial intelligence and machine learning algorithms cannot form part of a computer-implemented invention where they can be shown to have a 'technical effect'; they are just not patentable in and of themselves. Where they form part of platforms and applications that solve specific technical problems, then the success of a patent application improves significantly. In summary, a combination of copyright and patent protection should provide a good basis for protecting investment in artificial intelligence and machine learning in the UK.

Artificial intelligence is, of course, inextricably linked with the data it consumes and the financial services industry generates vast amounts of data. The data itself comes with a set of intellectual property protections – mostly confidentiality, sometimes copyright and, potentially, the sui generis database right. For example, look-up tables (databases accessed by software routines) are potentially protected by copyright in the structure of the database and by the sui generis database right protecting the extraction and reutilisation of the data contained in the database (provided the owner can show substantial investment in obtaining the data).

The database right is a powerful right, and while the protection ostensibly lasts for 15 years, each time substantial investment is expended in obtaining, verifying or presenting the contents of the database, a new database is likely deemed created and thus a rolling protection obtained. There has been some debate as to whether aggregations of data, for example, sensor or machine-generated data, can fulfil the 'substantial investment in obtaining' requirement of the database right. The debate continues as to where the threshold of effort lies. Irrespective of whether or not the contents of a database are protected by confidentiality or database rights, both can provide limitless protection. Because big data is becoming such an integral part of any business dealings, the UK competition authorities are sure to consider moves to counteract potentially monopolistic effects of vast datasets being controlled by relatively few market players.

Turning to blockchain technologies, similar issues are encountered: patent protection for spreadsheets is not available, and there will need to be some actual technical effect, similar
to software-enabled inventions. Copyright is the most common form of protection for blockchain, both proprietary and open-source. The basic building blocks of many blockchain technologies are open-source software codes, but those building on top of the originating technologies may want to protect their inventions through more commercial protections, such as more restrictive copyright and patent licensing.

ii Data protection

In the same way as for intellectual property, financial services technologies also test the existing legal framework around data protection, despite the General Data Protection Regulation (GDPR) being of very recent provenance.

The UK Information Commissioner’s technology priorities for 2019 include cybersecurity, artificial intelligence, big data and machine learning and online tracking technologies, all of which are highly pertinent to technologies within the financial services sector.

Big data analytics again poses difficulties for data protection law. Difficulties include running large numbers of algorithms against vast datasets to find correlations; the opacity of the processing; the tendency to collect ‘all the data’; the repurposing of data and the use of new types of data; not to mention the hurdles of distinguishing between data controllers and data processors. Clearly all of these activities have implications for data protection.26

The Information Commissioner’s Office is reaching out to partners as part of its Technology Strategy to better understand these technologies, and is seeking to establish a regulatory sandbox, drawing on the successful sandbox process that the FCA has developed. The sandbox is expected to enable organisations to develop innovative digital products and services, while engaging with the regulator, who will provide advice on mitigating risks and data protection by design.27

New blockchain technology also poses data protection challenges. There has been significant debate as to whether or not the hashed information contained on the blockchain could be considered personal information and, if it is, how the GDPR can be reconciled with the benefits of the blockchain being an immutable source of the truth without the need for trusted intermediaries. This question has yet to be resolved.

In addition to the GDPR, PSD2 includes a number of specific rules concerning the processing of personal data. For example, PSD2 provides for ‘explicit consent’ raising the question of whether this constrained the use of the various other bases for processing set out in the GDPR. The European Data Protection Board has clarified that it did not. ‘Explicit consent’ referred to in PSD2 is a contractual consent that is an additional requirement of a contractual nature. Payment services are always provided on a contractual basis between payment service user and payment service. There still needed to be a requisite basis for processing the data under the GDPR, for example, processing necessary for the performance of a contract to which the data subject is party.

VIII YEAR IN REVIEW

The year 2019 saw the publication of ‘Liability for Artificial Intelligence and Other Emerging Digital Technologies’, an expert report from the European Commission. Its findings are particularly pertinent to fintech, which has been an early adopter of AI and robo-advisers.

In particular, the report noted that a resolution to the question of who (in principle) is liable for the output of an AI tool is becoming increasingly urgent as powerful AI systems are being created. In the UK, these are likely to take the form of contract and tort-based claims specific to the facts of each case. While such claims may be complicated, the year ahead is likely to see the development of ways that the complexity might be addressed. For example, in the case of robo-advisers competing in the independent financial adviser/fund manager market, potential issues can arise in establishing a breach of duty of care given potential ‘black box’ problems. These issues might be addressed by focusing on the inputs and the outputs of the AI, for example, whether the investments match the instructions given. The report also concluded that, in the case of AI, it is not necessary to create a further category of legal personality, as the harm it causes should be attributable to existing legal persons or bodies.

Last year saw record investment in the UK fintech sector, with London attracting the biggest number of international investors, overtaking New York for fintech investment deals, which is underpinned by supportive regulation and an early adopting customer base.

The end of 2019 saw the signature of the UK–EU Withdrawal Agreement. Under the agreement, from 31 January 2020, the UK is no longer a member of the EU. Nevertheless, the parties agreed an implementation period where the UK continues to be subject to EU rules and remains a member of the EU Single Market and customs union. This allows the parties to continue their current relationship while a future trading relationship is negotiated. The implementation period is due to end on 31 December 2020, whether or not a trading relationship has been agreed.

IX OUTLOOK AND CONCLUSIONS

Much of the focus in the coming months will be on the outcome of the future trading relationship between the UK and the EU and how it affects the market based on the deal (or lack of it) reached with the remaining EU Member States.

When the implementation period has expired, whether firms will continue to be able to make use of existing passporting regimes will depend on the terms of the agreement over the future relationship between the UK and the EU.

The payments sector is the most likely to be affected by Brexit, given the strength and size of the UK’s banking sector relative to other jurisdictions. Indeed, as firms begin to make the most of the new markets created by PSD2, it was the UK that stood to gain most from those. However, a question now remains as to how much of that opportunity will be lost, despite the fact that, the rules will be transposed into the UK statute book so as to continue to be effective at least in the short term.

It will also be worth keeping one eye on the asset management industry in 2020. As wealth-tech providers including technologically advanced asset management solutions proliferate, the retail asset management industry looks set to face a regulatory shake-up by the FCA and Bank of England following issues with Neil Woodford’s investment funds and liquidity structuring. That could create the perfect environment for the wealth-tech firms to gain significant market share in the event that the FCA and Bank of England do recommend a repositioning of the market.
The UK is the third most connected country in the world, and maintenance of dataflows between the UK and the EU will be a priority in the forthcoming negotiations. The UK is keen to obtain an ‘adequacy’ decision as part of the future trading relationship – otherwise it will become a third country from the perspective of EU dataflows, and companies will have to put in place more cumbersome compliance mechanisms to govern these, such as binding corporate rules, EU standard contractual clauses or other approved arrangements.

From an IP perspective, the European Patent Convention is not directly linked to the European Union, so European patents should not be affected by Brexit. By contrast, Community Trade Marks are linked to membership of the European Union. Thus, once the transition period ends, Community Trade Marks will technically cease to have effect in the UK. However, the UK government has indicated that even if there are no deals with the EU they will permit Community Trade Mark registrations that are in force at the time of exit from the EU to be extended in to the UK so that pre-existing trade mark rights will not be lost. As for the sui generis database right, the government’s Regulatory Policy Committee states that the UK government’s preferred option is to maintain the status quo after Brexit so far as possible for UK database creators and consumers.28

Blockchain will continue to present challenges around applicable law, as it involves computers located across the globe. In cross-border decentralised blockchains, individual transactions will need to be analysed on a case-by-case basis.

28 Intellectual Property (Amendment) (EU Exit) Regulations 2018 and various impact assessments published by the Regulatory Policy Committee (RPC).
Chapter 27

UNITED STATES

Erin Fonte, Scott Kimpel, Carleton Goss, Brenna McGee and Patrick Boot

I OVERVIEW

Most experts acknowledge that the United States has one of the most complex financial regulatory regimes in the world. This is largely due to the two-tiered regulatory environment, where states and the federal government both regulate financial activity. Currently, there are five primary federal financial regulators and each state also has its own financial regulator. There are overlapping, inconsistent and, occasionally, contradictory financial regulations that companies with multi-state activities, including fintechs, must navigate. Without the availability of options such as ‘passporting’ licences from one jurisdiction to another (which are available in other regions of the world like the European Union), thoughtful and well-staged operating and licensing strategies for fintechs launching online or mobile products and services that will essentially be operating in all 50 states is critical. In addition to the geographic regulatory complexity, federal and state regulators are focused on licensing the underlying activities that fintechs engage in, which can trigger a whole host of other regulations (and other regulators) that fintechs must address. While federal and state regulators are committed and have been moving over the last several years to harmonising inconsistent and sometimes conflicting regulations, in the near term regulatory challenges will continue to exist in the US.

II REGULATION

i Licensing and Marketing

There are few fintech-specific licenses or regulations in the US at either the federal or state level. Instead, the regulatory regime that applies to a fintech company in the US depends on the activities that the fintech engages in and the products and services that it offers. Both federal and state regulators have made clear in regulations, guidance and enforcement actions that they are focused less on the channel of delivery of fintech services (e.g., online or mobile) and more on the underlying activities that a fintech engages in (e.g., payments, small-dollar lending, virtual currency). Regulators at the federal and state level have taken several enforcement actions in recent years against non-bank fintech companies, including enforcement actions involving alleged violations of federal securities laws (particularly with regard to initial coin offerings), insufficient data security practices and data breaches, failure to obtain necessary licensing, and unfair and deceptive acts and practices.

1 Erin Fonte and Scott Kimpel are partners, Carleton Goss is counsel, and Brenna McGee and Patrick Boot are associates at Hunton Andrews Kurth LLP. The authors wish to thank Rachael Craven, Mayme Donohue and Ryan Logan for their contributions to this chapter.
The regulatory regime and required licensing for fintechs is complex and can touch upon several federal and state regulatory and licensing issues, and many non-US fintech companies that seek to operate in the United States are often taken aback at the complexities of the US regulatory and licensing requirements. This is particularly true at the state level, where there currently is no option to obtain a licence in one state and then have that licence granted reciprocity for licensing in other states – a situation that contrasts strongly with the ability of EU countries to ‘passport’ certain licences in from one country to another. The complex nature and somewhat lengthy process of obtaining state licences in particular has been criticised as a barrier to entry and potential hindrance to innovation by non-bank fintech entities seeking to operate in the US.

By way of example, a fintech product such as a mobile wallet may trigger one or all of the following federal regulations, depending on its structure and the products and services offered: (1) Electronic Funds Transfer Act (EFTA) (and corresponding Federal Reserve Board Regulation E); (2) EFTA and ‘Regulation E Lite’ (which applies to the issuers of ‘access devices’ even if they are not the issuers of the underlying payment account); (3) truth-in-billing laws (if payments are charged directly to a consumer’s mobile wireless or mobile carrier account); and (4) Bank Secrecy Act (BSA) and anti-money laundering (AML) regulations and corresponding ‘know your customer’ (KYC) and customer identification programme requirements.

At the federal level, the only agency that has direct supervisory and regulatory authority over non-bank fintechs is the Consumer Financial Protection Bureau (CFPB). The CFPB regulates non-bank fintechs that provide financial products and services directly to consumers, and has the authority to enforce several consumer protection laws, such as EFTA (and corresponding Federal Reserve Board’s Regulation E), the Truth in Lending Act (and corresponding Federal Reserve Board’s Regulation Z), as well as the ability to take enforcement actions against the use of unfair, deceptive or abusive acts and practices by fintechs in marketing or providing their services. In addition, each federal functional regulator (the Federal Reserve, Office of Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC) and the National Credit Union Administration) also has its own rules on marketing that apply to the entities it regulates (and it is important for fintechs to be aware of these because of the ‘pass-through’ regulatory requirements discussed below). Generally, unfair, deceptive or abusive marketing practices are prohibited. An act or practice is unfair if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers and not outweighed by countervailing benefits to them or to competition. A deceptive act or practice involves a representation or omission that is likely to mislead a reasonable consumer in some material way. Section 1031(d) of the Dodd-Frank Act defines abusive conduct or activity as something that:

a materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or

b takes unreasonable advantage of:

• a lack of understanding on the part of the consumer of the material risks, costs or conditions of the product or service;
• the inability of the consumer to protect its interests in selecting or using a consumer financial product or service; or
• the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.
While the CFPB has, since 2011, further defined or clarified what constitute abusive practices through its enforcement actions, on 24 January 2020, the CFPB issued a policy statement regarding abusive acts or practices, stating that the CFPB will challenge the conduct that may be defined as abusive only when harm to consumers is judged to outweigh the benefits, and that the CFPB will seek monetary damages in the instance that an entity acts with a lack of good faith to comply with laws.

If a fintech’s products, services or activities involve providing investment advice or acting as a broker or dealer of securities, in general it must be licensed and regulated by the Securities and Exchange Commission (SEC) or the Commodities Future Trading Commission (CFTC), as applicable. Robo-advising services, which are a type of investment advisor activity, fall within this category.

Providing automated digital advisory or asset management services may constitute acting as an investment adviser. The critical inquiry as to whether the fintech entity would be deemed an investment adviser is whether, in connection with the product, the fintech will be providing advice to others regarding securities or issuing reports or analyses regarding securities. In addition to recommending individual stocks or bonds, providing advice about securities also includes advising on:

- market trends;
- the selection and retention of other advisers;
- the advantages of investing in securities versus other types of investments (e.g., coins or real estate);
- a selective list of securities even if no advice is provided as to any one security;
- the value of securities;
- asset allocation; and
- voting proxies.

Fintechs that engage in credit information services may be subject to the Fair Credit Reporting Act (FCRA). FCRA regulates the collection, dissemination and use of consumer information, including consumer credit information. To the extent that the fintech is supervised by a state or federal regulator, that regulator would be in charge of assessing and enforcing compliance with FCRA.

If a fintech qualifies as an insurance broker or underwriter, it is regulated at the state level by state insurance regulatory agencies. If a fintech makes loans, it may have to obtain state lender licences and be subject to oversight by state regulators that administer and oversee the licensing and ongoing activities of licensed entities, including consumer protection regulations.

If a fintech provides payments services, such as peer-to-peer money transmission or the payment of bills to third parties, and qualifies as a money services business, then it must register as a money services business with the US Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN), and must also obtain state money transmitter licences when required, which makes the fintech subject to ongoing state money transmitter licence renewals, reporting and examination. In some instances, a fintech may mistakenly believe that registering as a money services business with FinCEN takes care of registration as a licensed money transmitter with individual states. This is absolutely not the case; an entity must comply with both federal money services business registration and reporting as well as the state-level money transmitter licensing requirements. In addition, if a fintech believes that
it falls within the ‘processor exemption’ or ‘agent of the payee’ exemption contained in federal money service business registration requirements, it should be aware that recognition of such exemptions must be determined on a state-by-state basis.

A fintech company may acquire the necessary regulatory licences by creating a new business entity and applying for licences for that entity. Alternatively, a fintech company may acquire an entity that already has the category of licence desired or may partner contractually with such an entity to jointly provide the products and services (provided the fintech also follows the required ‘notification of change’ requirements for informing and gaining regulatory approval for a change in ownership of a licensed entity). While each strategy comes with its own advantages and disadvantages, many fintechs have found that in order to enter the market, they must partner with either a financial institution or other existing licensed entity.

Fintechs that partner with financial institutions to offer their products and services (which includes almost all fintechs that must gain access to the payment systems or maintain pooled or other bank accounts for clearing and settlement of transactions) are third parties partnering with the financial institution and fall within the financial institution’s obligations to perform due diligence, monitoring and oversight as part of its overall third-party risk management regulatory obligations. This gives rise to the concept of pass-through regulatory requirements where a financial institution must rely on and ensure that its fintech partner, as the primary point of customer onboarding and interaction, assists the financial institution in meeting its regulatory obligations, such as BSA and AML requirements, Office of Foreign Asset Control (OFAC) screening of new customers, Regulation E investigation and dispute resolution activities regarding consumer claims of unauthorised or fraudulent activities. In fact, federal functional banking regulators (the Federal Reserve, OCC, FDIC and National Credit Union Administration) have the authority to take enforcement actions directly against third-party financial institution fintech partners. The Federal Deposit Insurance Act contains provisions addressing enforcement actions against an institution-affiliated party, which includes in its definition any ‘joint venture partner, and any other person as determined by the appropriate Federal banking agency (by regulation or case-by-case) who participates in the conduct of the affairs of an insured depository institution’. There have been several joint FDIC and US Department of Justice investigations and enforcement actions that have included both fintechs and their financial institution partners.

Given the complexity of the US regulatory regime for fintechs, there has been widespread debate in the past several years in the US regarding the creation of a more comprehensive licensing regime for fintech entities. On 31 July 2018, after several years of discussion, the OCC announced that it would be accepting applications for special purpose national bank charters for fintech companies. Long anticipated by the fintech industry and opposed by multiple state regulators, the OCC fintech charter is viewed as a way to potentially alter the financial services landscape for non-bank fintech entities. For fintech companies serving customers in multiple states, the OCC fintech charter could reduce the administrative and compliance challenges posed by the existing patchwork of state licensing requirements. But applying for such charter could come at a steep cost because fintech companies would have to meet stricter, bank-like regulatory requirements associated with an OCC charter.

As of 1 March 2020, no fintech company had officially submitted an application to the OCC for the limited-purpose fintech charter, although a few are reportedly in pre-application discussions. The hesitation from fintech companies to apply for the new charter may be based on the heightened regulatory requirements, as well as a series of lawsuits the OCC is facing from state regulators and the Conference of State Banking Supervisors (CSBS), the nationwide
organisation of state financial regulators. Two sets of lawsuits have been brought by both the CSBS and Maria Vullo, the then Superintendent of the New York State Department of Financial Services. Both the CSBS and the New York State Department of Financial Services have criticised the OCC’s decision to permit limited purpose fintech charters as ‘lawless, ill-conceived, and destabilizing of financial markets’. In response, the OCC has said that it will vigorously defend its authority to grant national charters to qualified companies engaged in the business of banking.

However, even with the uncertainty and litigation regarding the OCC’s limited purpose fintech charter, there are several fintechs that are exploring or have applied directly for full national bank charters or state industrial loan company charters (ILCs) that would be jointly regulated by the state granting the ILC charter and the FDIC. Applications for ILCs have been met with criticism from financial institution trade associations such as the American Bankers Association and the Independent Community Bankers Association of America (ICBA), that each claim ILCs are a loophole fintechs are attempting to exploit to get into banking. In March 2019, ICBA put out a White Paper entitled ‘Industrial Loan Companies: Closing the Loophole to Avert Consumer and Systemic Harm’. In the White Paper, ICBA raises concerns that there are regulatory blindspots in the ILC model that pose a threat to safety and soundness as well as stating that ILCs are the functional equivalent of full-service banks and that commercial company ownership of ILCs will effectively combine banking and commerce, contrary to long-standing American economic policy.

However, current FDIC Chairman Jelena McWilliams has indicated a willingness for the FDIC to look at and evaluate ILC charter applications. She has commented that issues of capital and profitability are key themes in the FDIC’s interactions to date with fintech companies seeking banking charters, and that conversations about regulatory capital – which must be at 8 per cent by the third year – have been cumbersome as the FDIC has been educating fintechs that ‘capital doesn’t equal equity’. Additionally, the FDIC has been evaluating the potential effects of fintech ILC applicants’ profitability on the deposit insurance system, and the agency is also reminding applicants to focus on how they are going to meet community needs in order to satisfy that element of the FDIC’s ILC application.

A fintech that desires to operate in the US and wants to explore obtaining a financial institution charter must carefully consider whether its contemplated activities would require it to be licensed by a state or federal agency, as well as whether the costs and other burdens associated with such a licence would be cost prohibitive.

On 31 July 2018, the US Department of the Treasury (the Treasury) released a report on ‘Non-bank Financials, Fintech, and Innovation’ (the Fintech Report), its fourth and final report on the US financial system pursuant to Executive Order 13772. Many of the Treasury’s recommendations would have a positive impact on creating a national and state regulatory environment to foster innovation in financial services, and the Fintech Report called specifically for (1) aligning the US regulatory framework to combat unnecessary fragmentation and addressing new business models enabled by new financial technologies; (2) updating activity-specific regulations across a range of products and services offered by non-bank financial institutions; and (3) promoting agile regulation and responsible experimentation. Several US federal regulators have launched ‘offices of innovation’ or similar units within their organisations, such as the OCC’s Office of Innovation and the FDIC’s FDITech innovation lab. In addition, the Federal Reserve has recently held a series of ‘fintech innovation office hours’ across the country to meet with banks and companies engaged in emerging financial technologies. While these initiatives do not provide all the functionality
and safe harbour environment that, for example, the UK’s Financial Conduct Authority’s (FCA) ‘Innovation Hub’ regulatory sandbox where fintechs can get feedback from the FCA on product design and compliance issues does, US federal regulators are taking a more proactive and hands-on approach to understanding technology, products and services that non-bank fintechs are developing and seeking to offer.

The Fintech Report also called for harmonising state regulations, stating that for several years running, non-bank fintechs have raised concerns about the lack of regulatory harmonisation across US state-based regulatory regimes, particularly on money transmission and lending activities. An online or mobile fintech start-up could potentially reach customers in all 50 states upon launch, and with that national, multi-state reach come significant regulatory and licensing requirements and costs if the fintech start-up’s activities were to require state level licensing (and also some costs to determine whether licensing is even required or not).

The Fintech Report did not recommend complete pre-emption of state laws and regulations, but instead that state regulators should strive to achieve greater harmonisation. The Treasury suggested states should consider drafting model laws that can be uniformly adopted, and also applauds states’ current efforts to streamline licensing requirements and coordinate examinations. For example, the Treasury specifically supports Vision 2020, an effort by CSBS to improve state regulation by harmonising the multi-state supervisory processes and redesigning the Nationwide Multistate Licensing System (NMLS). While there has not been much movement on states adopting reciprocal licensing regimes (for example, where a fintech could get a licence in California and then get reciprocal licensing in all other states), there have been significant advances made in streamlining and harmonising the state money transmission licensing process. The Multistate Licensing Agreement came out of the Vision 2020 initiative in 2018, launching with seven participating states. As of 1 March 2020, there are 27 participating states (11 of which are Phase 1 only states). Under this programme, one state regulatory agency reviews the common licensing requirements across all states such as: business plan; direct and indirect owners, including background checks; and financial information and compliance with the AML provisions of the BSA. These important components of any money transmitter entity represent a large part of an application review workload. The state communicates the review, called a certification, to all other participating states that have agreed to accept the findings (the Phase 1 Review). Each state then reviews the remaining, state-specific elements, and licences follow this Phase 2 review. The purpose of the Multistate Money Services Businesses Licensing Agreement (MMLA) Program (as administered under the NMLS) is to create a more efficient money transmitter licensing process among state regulators. While much work is still to be done on the state harmonisation front, moving from seven to 27 participating states in two years is good progress.

ii Cross-border issues

Generally, if any entity, domestic or foreign, seeks to conduct regulated activities in a US jurisdiction, it must maintain the appropriate licence or registration, even if the entity is already licensed to conduct the same or similar activities in another jurisdiction or country. There is no ‘passporting’ in the US of licences or registrations into the US from a foreign jurisdiction, and there is no ‘passporting’ state licences or registrations into other states (although there are ongoing efforts to streamline and harmonise state regulation as discussed.
above). However, in the US, the concept of federal pre-emption renders inapplicable certain state requirements that may apply to the provision of financial services if those services are provided by a federally licensed and regulated financial entity.

Each jurisdiction has its own rules with respect to physical presence requirements. Generally, foreign companies may provide financial services in any US jurisdiction by registering with the appropriate regulator or, if necessary, with the Secretary of State or tax authorities of the jurisdiction. Some jurisdictions even permit their own licensed entities to maintain some or all of their substantive business operations outside of the jurisdiction. For US financial institution charter applications and state money transmitter applications, there are strict criminal background checks, financial records and fingerprinting requirements for owners, major shareholders, directors and executive officers.

All US persons are required to abide by federal trade and sanctions programmes. These programmes are managed by the US Department of Treasury’s OFAC. Additionally, the Committee on Foreign Investment in the United States (CFIUS) is an interagency committee authorised to review certain transactions involving foreign investment in the United States and certain real estate transactions by foreign persons, in order to determine the effect of such transactions on the national security of the United States.

III DIGITAL IDENTITY AND ONBOARDING

i Digital identity

There is currently no generally recognised digital identity in the United States. While the US Department of Commerce National Institute of Standards and Technology (NIST) has issued technical requirements for digital identity services, the guidelines are only mandatory for the federal government and voluntary for the private sector. Nevertheless, the NIST guidelines are generally seen as setting the standard for the direction of any potential federally recognised digital identity.

The Fintech Report discussed above includes two recommendations focused on the creation of a national digital legal identity and encourages private and public sector stakeholders to leverage the NIST guidelines to develop trustworthy digital identity products and services. The Fintech Report describes digital legal identity as using electronic means to unambiguously assert and authenticate a real person’s unique legal identity, and highlights two essential components of digital identity systems: identity proofing, enrolment, and credentialing; and authentication. Federation is a potential third component that would allow identity to be portable. Another recommendation in the Fintech Report urges the Office of Management and Budget to fully implement the long-delayed government federated identity system. As emphasised by the Treasury, the creation of a nationwide digital legal identity framework will ultimately require close collaboration between the government and the private sector in the United States.

ii Digital onboarding

Fully digitised onboarding of clients is the method by which many digital-only fintechs have been able to achieve staggering growth in the number of customers in relatively short time frames. While digital onboarding poses numerous risks, regulators in the US acknowledge the benefits for providing access to innovative products and services. Digital onboarding again raises the concept of pass-through regulatory requirements discussed above, where fintechs must ensure specific regulatory obligations are met, namely BSA, AML and OFAC screening.
Unlike the EU, where fintechs are able to rely on specific digital onboarding regulations such as the new European Anti-Money Laundering Directive, digital onboarding in the US requires compliance with the standard Customer Identification Program (CIP) and customer due diligence (CDD) requirements to ensure BSA and AML compliance – CIP requirements involve verifying the identity of customers while CDD requirements involve identifying and verifying the identities of beneficial owners of legal entity customers.

As part of a comprehensive CIP, fintechs partnering with US financial institutions to open accounts for customers must obtain the following information before opening an account: name, date of birth (for natural persons), address, identification number (e.g., a tax identification number) and a government-issued document bearing a photograph for a natural person or government-issued documentation certifying the existence of an entity. Other than various additional CIP requirements, fintechs may also be required to establish comprehensive CDD programmes. Additional specific onboarding requirements vary greatly based on the underlying product or service being offered. For example, prepaid products will have far less strict requirements than mortgage products. There are a variety of companies, such as Verafin (anti-fraud services) and Okta (single sign on and multi-factor authentication services), providing identity verification solutions to the financial sector that fintechs may be able to leverage in bringing new products or services to market.

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

There are a variety of different digital marketplaces operating in the US, from more traditional marketplaces like eBay, Amazon, Mercari and Etsy that offer diverse goods from a variety of sellers, to newer niche marketplaces like Uber and Lyft (for ridesharing), Airbnb and VRBO (for home rentals), and Grubhub, DoorDash and Postmates (for food delivery). Generally speaking, these marketplaces for goods and services are not regulated as fintech companies in the US. Most of these marketplaces are only regulated based on their underlying goods or services. For example, Uber and Lyft are subject to the same regulations as taxis in many US jurisdictions. These digital marketplaces are generally not subject to fintech regulations because either the funds for the purchase of goods flow through a separate payments company – for example, payments for eBay purchases have historically been handled by PayPal – or the marketplaces do process payments but do so under an exemption to fintech regulation (such as ‘agent of the payee’) or only accept credit card payments, which do not require fintech licences in the US. However, in recent years some of these marketplaces have chosen to register with FinCEN as money services businesses (MSBs) and obtain state money transmission licences to able to process a wider variety of payments. For example, both Airbnb and Amazon have created separate subsidiaries (Airbnb Payments, Inc and Amazon Payments, Inc, respectively) to be able to offer more payments services, including processing payments for other merchants and making faster payments to their sellers. For those marketplaces that choose to cross over into fintech and payment services, the whole host of fintech regulations, as discussed above, will apply.

Digital marketplaces specifically for buying, selling and trading digital assets or cryptocurrencies are subject to significant regulations in the US. As discussed in detail below, the underlying assets are subject to a range of regulations from a variety of different state and federal regulators. In addition, the marketplaces themselves are also regulated. In some cases, they are MSBs that are registered with FinCEN and licensed as a state money transmitters: for example, both Coinbase and CoinZoom are digital currency trading platforms that are
subject to money transmission regulations in some US jurisdictions because of their handling of crypto or fiat currencies or both. Gemini Trust Company is another digital currency exchange that is a regulated fintech company, although it is primarily regulated by the New York State Department of Financial Services as a New York trust company, rather than as an MSB. As discussed below, the New York State Department of Financial Services also regulates cryptocurrency marketplaces under its special ‘BitLicense’ regime; fintech entities including Ripple, BitPay, Coinsource and Robinhood have all been awarded BitLicenses in New York.

While a ‘collective investment scheme’ is a term of art used in the UK, colloquially collective investment schemes in the United States may refer more broadly to pooled investment vehicles or funds, such as ‘public’ investment funds (e.g., mutual funds) or ‘private’ investment funds (e.g., a private equity fund, real estate fund or hedge fund). These funds are generally regulated by the SEC, but may also be subject to the regulation of the CFTC, Financial Industry Regulatory Authority (FINRA), National Futures Association and United States state regulatory agencies. Depending on the structure of the funds and the nature of the funds’ holdings, these funds and their managers or sponsors may be subject to the Investment Company Act of 1940, the Securities Act of 1933, the Investment Advisers Act of 1940, the Securities Exchange Act of 1940 and the Commodity Exchange Act.

In recent years, peer-to-peer lending, social-lending and crowd-lending have become popular alternatives to standard bank loans in the United States. However, many of the consumer protection laws applicable to traditional loans may also apply to loans made via these marketplace lending platforms, including the Truth in Lending Act, Equal Credit Opportunity Act and Fair Debt Collection Practices Act. The regulators primarily responsible for enforcing these consumer protection laws include the CFPB and the Federal Trade Commission. Depending on the particular business model, marketplace lenders may also be regulated by the Federal Reserve, FDIC, and the OCC. In addition, marketplace lenders may be subject to state consumer protection laws, including laws prohibiting unfair, deceptive, or abusive acts and practices, and may be subject to state licensing requirements to act as a lender, broker, debt collector, or solicitor.

Payments services – including traditional peer-to-peer (P2P) funds transfer companies like Western Union and MoneyGram and new fintech entities like Venmo and TransferWise – are heavily regulated in the US and are required to both register as a money services business with FinCEN and also obtain state money transmitter licences. As mentioned above, some fintechs mistakenly believe that registering as an MSB with FinCEN is sufficient to operate as a payments service in the US; that is not the case, as state-level money transmitter licences are also required. Furthermore, payments services must obtain a licence in each state in which they intend to operate because the US currently lacks a reciprocity or passporting option as in Europe. The lack of passporting or reciprocity in the US is particularly notable because obtaining all state money transmission licences is extremely burdensome, often taking years and costing hundreds of thousands of dollars. Although each state generally has the same application requirements, they are not uniform and fintech entities cannot submit one standard application to all states. Instead, they must apply to each state individually. State money transmission licensing requirements include, but are not limited to, paying an application fee, obtaining a surety bond or other form of security, having a significant net worth (usually around $500,000), submitting audited financial statements, and having shareholders and principals of the entity undergo fingerprinting and background checks. While the current US licensing regime is onerous, state regulators are taking steps towards licence reciprocity and a standardised application process. As discussed above, the states have
made significant strides towards a standardised licensing process with the Multistate Money Services Businesses Licensing Agreement Program and state regulators continue to work toward their goal of an integrated, 50-state system of licensing and supervision for money transmitters by the end of 2020.

Unlike under the EU Revised Payment Services Directive, there is no law or regulation in the US directly requiring financial institutions to share customer data with fintech entities. Although Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) requires banks and other financial service firms to make customers’ financial data available to the customer in a usable form, no promulgated rules define what ‘usable form’ means or identify sanctions for financial institutions that limit what information they share. While the CFPB has the authority to pass regulations on data sharing under Dodd-Frank, it has opted not to do so thus far. In October 2017, the CFPB published a set of nine non-binding Consumer Protection Principles that affirmed consumers’ ownership rights over their financial data, but they did not mandate how financial institutions must share that data with consumers and third parties in the US. However, new rules from the CFPB may be on the horizon. In February 2020 the CFPB held a symposium on consumer access to financial records and Section 1033 of Dodd-Frank. The CFPB stated that it specifically organised the symposium to solicit feedback to guide the agency in its policy development process, therefore rules requiring financial institutions to share customer data with third parties are likely forthcoming. Additionally, the CFPB announced support of the work being pursued by the Financial Data Exchange (FDX), a consortium of leading financial institutions and fintechs, focused on creating a global standard for data sharing through the development of the FDX application programming interface (API).

V DIGITAL ASSETS

After more than a decade in the market since Bitcoin first went live on 3 January 2009, regulatory uncertainty and a patchwork of evolving legal frameworks continue to impact the evolution of cryptocurrencies, security tokens and other digital assets in the US. At the federal level, the SEC, the FinCEN, the Internal Revenue Service (IRS), and the CFTC have taken turns to issue administrative guidance and enforcement actions to shape the regulatory landscape for this new asset class. In addition, a majority of states have either enacted or proposed formal legislation related to digital assets or the underlying blockchain technology, with certain states adopting extensive legislative frameworks designed to attract blockchain and crypto entrepreneurs to their jurisdictions. State securities regulators and private plaintiffs are also involved, mostly through enforcement or civil action against potential fraudsters. At the core of all regulation on digital assets is the cumbersome effort to fit digital assets into existing legal frameworks for more traditional assets like securities, commodities and currencies.

i Digital assets as securities

Since it first published the DAO Report on 25 July 2017, the SEC has consistently applied the 75-year old definition of an investment contract using the ‘Howey test’ to determine which digital assets are securities and most recently summarised its position in 2019 in the Framework for ‘Investment Contract’ Analysis of Digital Assets (the Digital Asset Framework). Under the Howey test, a digital asset is an investment contract and, therefore, a security, when there is the investment of money in a common enterprise with a reasonable
expectation of profits to be derived predominantly from the efforts of others. The Digital Asset Framework applies the prongs of the Howey test to common characteristics of digital assets and, importantly, also acknowledges the possibility that a digital asset can evolve over time and cease to be deemed a security under certain circumstances. With the SEC’s framework heavily dependent on the facts and circumstances of each digital asset, those seeking to issue a security token or new cryptocurrency are faced with the choice of either complying with SEC registration requirements or seeking no-action relief that they are not issuing a security. To date, the SEC has only granted two such no-action letters and the companies seeking to register their digital tokens in reliance on Regulation A have faced heightened scrutiny and questioning from regulators with only two offering statements being made effective.

In an attempt to modernise the SEC’s approach, SEC Commissioner Hester Peirce (whose favourable public statements on digital assets have earned her the nickname, ‘Crypto Mom’) recently released a model rule on digital token sales in connection with a public speech entitled, ‘Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization’. Commissioner Peirce’s proposed solution to the current regulatory uncertainty would revolutionise the crypto markets because it proposes a three-year safe harbour from SEC registration while a development team builds out a functional, decentralised network supporting the digital token. In Commissioner Peirce’s view, once a network cannot be controlled or unilaterally changed by any single person, entity, or group of persons or entities under common control, the token that operates on that network will not look like a security. Accordingly, upon the conclusion of the three-year period, the model rule provides that the development team would be required to determine whether token transactions involve the offer or sale of a security under the Howey test. Nevertheless, Commissioner Peirce’s model rule exists wholly outside of the SEC’s formal rulemaking process and formal action on her proposal is not expected.

In 2019, the SEC and FINRA issued the Joint Statement on Broker-Dealer Custody of Digital Asset Securities (the Joint Statement), in which ‘digital asset’ refers to any asset that is issued and transferred using distributed ledger or blockchain technology, and a ‘digital asset security’ is any digital asset that is also a security for purposes of the federal securities laws. The Joint Statement discussed the application of digital asset securities to the SEC’s Customer Protection Rule, which, among other things, requires broker-dealers to hold customers’ securities at a ‘good control location’, which is typically a third-party custodian like a trust company. The Customer Protection Rule deems banks a good control location; however, FDIC-insured banks are currently restricted from providing custody for digital asset securities. As a result of this hole in the market, Wyoming recently passed legislation creating special purpose depository institutions (SPDIs), which are banks that receive deposits and conduct other incidental activities, including fiduciary asset management, custody and related activities, focusing heavily on digital assets. In addition to providing a good control location for the purposes of the Customer Protection Rule, SPDIs are also designed to ensure digital assets are protected in federal bankruptcy proceedings. Other states, like Colorado and Missouri, are working towards creating similar digital asset banking institutions.

Digital assets as virtual currencies

In 2013, FinCEN issued interpretive guidance clarifying its position that the BSA applies to persons creating, obtaining, distributing, exchanging, accepting or transmitting virtual currencies. FinCEN classifies such individuals as exchangers or administrators of virtual currencies, which are treated as money transmitters required to register as MSBs. Money
transmitters are required to comply with the BSA obligations that apply to MSBs, including: registering with FinCEN; developing, implementing and maintaining effective AML and KYC programmes; filing suspicious activity reports and currency transaction reports; and maintaining certain other records. In the years since its initial 2013 guidance, FinCEN has issued numerous civil money penalties against cryptocurrency and digital asset enterprises for violation of the BSA.

The IRS issued the agency’s first crypto-related guidance in 2014 formally defining a virtual currency as ‘a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value’. According to the IRS, Bitcoin is a convertible virtual currency because it can be digitally traded between users and can be purchased for, or exchanged into, US dollars, euros and other real or virtual currencies. The IRS treats virtual currencies as property and applies the general tax principles applicable to property transactions to transactions using virtual currency. This means every sale or exchange of a virtual currency must recognise capital gain or loss on the sale. The IRS used its subpoena power in 2018 to identify and collect unpaid federal capital gains taxes from thousands of individual customers of the cryptocurrency exchange, Coinbase. Towards the end of 2019, the IRS released additional cryptocurrency tax guidance, including Revenue Ruling 2019-24 as well as a list of 45 frequently asked questions, to assist taxpayers to better understand reporting obligations for specific transactions involving virtual currencies. Revenue Ruling 2019-24 focuses on hard forks of virtual currencies and how hard forks impact whether an individual has received gross income for tax-reporting purposes. With what is considered a blow to the spread of cryptocurrencies for everyday use, such as purchasing a cup of coffee, the IRS refused to create a de minimis exemption for transactions below a certain threshold. Absent clear instructions from Congress, the IRS is adamant that it will not create a de minimis exemption for virtual currencies since there is no such exemption for other types of property.

Since 2015 the CFTC has exerted regulatory control over virtual currencies as commodities under the Commodity Exchange Act that can be purchased on the cash or spot market or through initial coin offerings (ICOs). The CFTC exercises its general anti-fraud and manipulation enforcement authority over virtual currencies under the authority of the Commodity Exchange Act. Summarising its position, LabCFTC, the CFTC’s fintech group released ‘A CFTC Primer on Virtual Currencies’ in 2017 and the CFTC has taken numerous enforcement actions against bad actors in the virtual currency markets. Additionally, federal courts have upheld the CFTC’s interpretation that virtual currencies are commodities within its regulatory jurisdiction.

New York State has created its own regulatory regime for virtual currencies and requires anyone engaging in any of the following to obtain a special licence called a BitLicense: virtual currency transmission; storing, holding or maintaining custody or control of virtual currency on behalf of others; buying and selling virtual currency as a customer business; performing exchange services as a customer business; or controlling, administering or issuing a virtual currency. Since the BitLicense was first required in 2015 until the end of 2019, the New York Department of Financial Services issued fewer than 25 BitLicenses.

State and federal governments will continue to develop rules and regulations as the digital asset industry matures. It can be expected that federal agencies will issue new and revised rules as their understanding of cryptocurrency, security tokens and blockchain technology evolves. The SEC and CFTC may also turn to Congress in order to request expanded powers to account for the vast changes occurring in the industries they regulate. Lawmakers are already becoming increasingly active as over 20 pieces of legislation will be
considered by Congress in 2020, covering a wide range of digital asset and blockchain policy. It remains to be seen whether the US can strike the proper balance of protecting the public without pushing investment in the technology to other jurisdictions. Industry participants need to continue working together with experts to avoid running afoul of rules or regulations in the increasingly complex and rapidly evolving regulatory environment.

VI OTHER NEW BUSINESS MODELS

i Self-executing ‘smart’ contracts

Self-executing contracts, or ‘smart’ contracts, are subject to general contract law and are legally permissible provided the particular contract satisfies the elements of a standard contract under US law. The enforceability and interpretation of contracts is generally a matter of state law in the US. Several states have enacted statutes aimed at ensuring smart contracts are granted the same legal validity as standard contracts, but there has yet to be any case law interpreting smart contracts in a commercial, or any, scenario. While smart contracts are technically permitted, the specific legal framework will depend on a variety of factors, such as the subject matter of the contract, and significant uncertainty remains around how smart contracts will ultimately be interpreted by courts. Until a consistent legal framework is developed, parties wishing for a smart contract to be interpreted as intended would be well advised to enter into a corresponding standard textual contract that courts can more easily understand in evaluating the enforceability of the smart contract counterpart.

ii Artificial intelligence in financial products

The CFPB has publicly supported the use of artificial intelligence (AI) and machine learning in financial products and services. AI has already been deployed by financial institutions through the use of regulatory technology products for BSA/AML compliance and OFAC screening, and is increasingly being used in lending and credit underwriting analysis and decisions. As it currently stands, financial products and services leveraging AI are subject to the existing regulatory framework of the underlying product or service. The uncertainty around how AI fits into the complex US financial regulatory framework is often cited as the cause of the lack of proliferation of AI-enabled financial products and services. Nearly all of the federal financial regulators have launched an office or programme aimed at financial technology innovation and facilitating adoption of beneficial AI and related technologies in the financial sector – these new offices include those of the CFPB and FDIC mentioned in Section II, as well as the OCC’s Office of Innovation, the CFTC’s LabCFTC, and the SEC’s FinHub. The CFPB has been particularly active in encouraging companies to engage in responsible testing of innovative technologies by creating various sandboxes and safe harbours, but the fact that many financial activities are also subject to overlapping state regulations complicates the agency’s efforts to provide companies with meaningful relief at this time. Central to regulatory issues regarding the use and deployment of AI in financial services, and also what is central in regulators’ review of AI in certain heavily regulated areas such as credit scoring and underwriting for lending, is how companies can explain the methodology and operation of an algorithm underlying the AI product, and also how the financial institution can provide regulators with a black-box test version of their AI to allow regulators to run independent testing, analysis and validation of AI technology (without compromising the underlying IP and proprietary elements of the AI algorithm or process).
iii Cannabis fintechs

The US currently has a complicated problem with respect to cannabis, which includes both marijuana and hemp. Although the majority of states have legalised hemp (and cannabidiol products derived from hemp) and some forms of medical marijuana, and many other states including California and Colorado have legalised recreational marijuana, at the federal level marijuana remains an illegal drug. This conflict between state and federal law has left cannabis-related entities in a difficult position, especially when it comes to payments. Some relief was provided at the federal level through the farm bill that became law in 2018 removing hemp from the controlled substances list and making it an ordinary agricultural commodity, but the same is not true for marijuana (which is defined as cannabis with more than 0.3 per cent THC). Marijuana, while legal at some level in many states, remains classified as an illegal substance at the federal level and has resulted in state-licensed cannabis-related entities being unable to access the banking system. This means that the vast majority of cannabis-related payments in the US are made in cash, both by consumers purchasing cannabis and companies making business-to-business payments, including to suppliers, landlords and taxing authorities. States, as well as public and private organisations, have urged the federal government to address this systemic problem, but so far little meaningful progress has been made. This conflict between states and the federal government has led to a proliferation of fintechs specifically targeted at addressing the financial issues faced by legitimate cannabis companies. Some of these fintechs attempt to address consumer-related payments issues, while others focus on business-to-business payments. Approaches for offering payments outside the traditional financial system include fintechs based in cryptocurrencies and digital assets, marketplaces for bartering and trading goods and services, and closed-loop stored value and mobile wallets specific to the cannabis industry. Despite general bipartisan consensus at all levels of the government that these cannabis-focused fintechs are providing vital solutions, fintechs operating in this space remain in a grey area as far as the law is concerned and need to work closely with expert legal counsel to ensure they are not exposed to significant legal liability.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

i Intellectual property, technology and data ownership issues

Owing to the fact that fintech products and services involve not only fintech-specific technology, software and user interfaces, but also mobile and online technology (not to mention a great many hosted services, cloud computing and software-as-a-service in the background), there are several intellectual property (IP) issues and potential claims that can arise for developers and users of fintech technologies.

When developing their products and technologies, fintech companies may believe that they have created a new and novel process or computer technology that could rise to the level of a patentable invention. The challenge of patenting financial services technology in the current environment is that court decisions over the past several years have narrowed the type of technology that is eligible for patenting. In 2014, the US Supreme Court issued what is commonly referred to as the Alice decision, which set forth a two-step eligibility test. If an invention is directed to a patent-ineligible abstract idea under the first step, the second step determines whether the patent’s claim (which places the public on notice of

2 Alice Corp Pty Ltd v. CLS Bank International.
the scope of the patentee’s right to exclude) recites elements that transform the abstract idea into a patent-eligible invention. Courts have generally applied this test to determine that the mere use of commercially available computing devices and software to implement an abstract concept is ineligible for patent protection. For instance, the use of a standard computer system to implement an escrow service for financial transactions was deemed in the *Alice* case to be ineligible for patent protection. However, a court might determine that the use of an innovative database technology to more efficiently conduct various aspects of financial transactions could transform abstract ideas relating to financial transactions into a patent-eligible invention. While it is difficult to predict with certainty whether an invention may be patent eligible, fintechs should confer with patent counsel to obtain guidance that will allow a well-informed decision to be made. Fintechs should be aware that business models or proprietary operations carried out by standard software may not be enough to seek a patent.

Fintechs should consider taking steps to protect their developed technologies in terms of copyright protection. Copyright protection extends to software code and certain works within software applications (like user interfaces and original text or content). More precisely, copyright protection extends to the source code, as the expression of the idea underlying the software, whereas the idea itself, or the function of the software, is not eligible for copyright protection. For this reason, copyright grants protection against the copy or use of the source code, but does not prevent third parties creating different source codes in order to replicate the functionality of a fintech software. If a fintech company is going to develop software utilising third-party software, the associated licence grants and restrictions from the licensing third party must be taken into account. And if the third-party software involves open-source software, and the fintech’s development consists of a ‘derived work’ resulting from a modification to that existing open-source software, it is possible that a ‘copyleft licence’ governing the open-source software may contain an obligation to distribute the derivative software under the same open-source licence, disclosing and making available to the public the source code.

As an alternative to obtaining a patent, a fintech may be able to maintain confidential information that provides an economic advantage over competitors as a trade secret. While patent law is premised on granting a temporary right to exclude others in exchange for the public disclosure of an invention, trade secret law provides an avenue for obtaining protection for economically valuable information such as a formula or algorithm. Trade secret protection presents its own set of challenges. If a trade secret holder fails to maintain secrecy or if the information is independently discovered, becomes released or otherwise becomes generally known, protection as a trade secret can be lost. For those reasons, it is important to enter into appropriate contractual arrangements that provide for the protection of trade secrets, including non-disclosure agreements and also specific contractual language such as IP and proprietary ownership and confidentiality provisions.

Finally, the fintech company will also want to take additional measures to preserve IP rights in distinctive names and other signifiers, such as logos, brand names and domain names to preserve brand awareness and guard against potential confusion. Registration of trademarks, design logos, brand names and domain names can prevent others from using those items that may be confusingly similar to the fintech company, helping to protect name and brand identity as well as position and recognition in the marketplace.

The fintech company should develop and deploy a comprehensive strategy for IP development and ownership from product development through product launch and scale. First, the fintech company should ensure that its agreements with employees and independent contractors that may be performing development work contain ‘work made for
hire’ or similar contractual language establishing that (1) the fintech owns all IP developed for it, (2) that employee or independent contractor acknowledges inventions, works or other intellectual property made or created by the employee or independent contractor during the term of employment or engagement are owned by the fintech, and (3) that the employee or independent contractor will take all necessary steps and complete any required documentation in order to assign those IP rights to the fintech. This will ensure that the fintech owns all of its IP, whether or not it chooses to explore any or all of the IP protection strategies described above.

With regard to third-party service provider agreements that the fintech may enter into for development or operation of the fintech services (such as hosting agreements, software-as-a-service agreements, agreements for identity verification services, etc.), the fintech will want to make sure that it is preserving the fintech’s IP rights while also acknowledging and recognising the rights of the third-party licensor of the software or services. For example, the fintech may grant a limited licence to a software or service provider to use anonymised and aggregated data (incapable of being reassociated with an individual) for the service provider to monitor their service performance, fix bugs, or offer new products or services to the fintech. The fintech will want to establish via contract that it owns all of its own and its customers’ data, and may want to limit or prohibit the extent to which the service provider can use the fintech’s information or data to sell new or improved products or services to others, and the fintech will want to prohibit a third-party service provider from selling any of the fintech or fintech customers’ data to third parties (and this prohibition and related analysis ties into the privacy and data security issues discussed below).

Finally, in customer-facing agreements, fintech providers will want to include robust provisions for confidentiality, intellectual property ownership, end-user terms of licensing and use (including allowed and prohibited activities under the licence), and may also want to disclaim all warranties of non-infringement or disclaim any liability or indemnification for third-party claims of infringement. In addition, the customer-facing agreements are also the appropriate place to obtain consumer or business-end customer consent for data collection, data usage by the fintech and specific permission to use fintech customer information in product improvement or data monetisation initiatives (all subject to the privacy and data security laws, rules and regulations highlighted below).

ii Privacy and data protection

In the United States, there is no overarching privacy law that applies broadly to all businesses. Rather, the Gramm-Leach-Bliley Act (GLB) is the primary federal privacy law that regulates the activities of fintech firms. GLB applies to the use and disclosure of any non-public personal information (NPI) by a financial institution. NPI includes any personally identifiable financial information that either (1) is provided by a consumer to a financial institution, (2) results from a transaction or service with the financial institution or (3) is otherwise obtained by the financial institution. The term ‘financial institution’ is broadly defined to include any entity that is significantly engaged in financial activities such as lending funds, servicing loans or transferring money. GLB is implemented by two distinct rules: (1) the Privacy Rule, which requires financial institutions to provide privacy notices to their consumers and customers and offer them an opportunity to opt out of certain disclosures of their NPI; and (2) the Safeguards Rule, which requires financial institutions to ensure the security and confidentiality of NPI through the development of a written information security programme. A wide variety of federal regulatory agencies have
United States

rulemaking and enforcement authority over financial institutions (and that can result in pass-through regulatory requirements to financial institution fintech partners), but fintech firms themselves would most likely be directly regulated by either the FTC or the CFPB with regard to privacy and data protection.

In addition, several states, such as California and New York, have enacted financial privacy or cybersecurity laws and regulations that may apply to fintech firms and are more stringent than GLB. For example, California’s new law, the California Consumer Privacy Act (CCPA) recently came into effect on 1 January 2020. CCPA does not apply to personal information ‘collected, processed, sold, or disclosed pursuant to’ GLB or the California financial privacy statute, but it does apply to any other personal information financial institutions collect that would not be considered NPI, such as the personal information of a financial institution’s employees.

On top of GLB, several other important federal and state laws and regulations for fintech firms to bear in mind and comply with include: (1) the federal Fair Credit Reporting Act (FCRA), which regulates the use and disclosure of consumer reports; (2) the federal Red Flags Rule, which requires financial institutions and creditors to develop, implement and update a written identity theft prevention programme to detect and respond to red flags that might indicate identity theft; (3) the federal Affiliate Marketing Rule, which limits the sharing of certain information among affiliated entities for marketing purposes; (4) if the fintech will be interacting with children, the federal Children’s Online Privacy Protection Act, provisions of the CCPA that apply to opt-in requirements for sale of data for children aged 13–16 (and parental opt-in consent for children 13 years and younger), and other California and additional state privacy laws that apply to children under the age of 18; and (5) the federal Health Insurance Portability and Accountability Act (if the fintech will be interacting with healthcare data).

In addition to laws that are straightforward in their applicability, other federal and state privacy and data protection laws may be triggered based on the type of security processes, procedures and tools fintechs deploy in their product offerings. For example, a fintech that utilises biometric recognition or verification tools through a mobile device must comply with state specific laws on biometric identification and information. The number of biometric privacy class actions has increased in recent years, with the decades-old Illinois Biometric Information Privacy Act (BIPA) continuing to pose the greatest concern to companies. While BIPA remains the only biometrics legislation to date in the US that provides for a private right of action, five other states (Texas, Washington, California, New York and Arkansas) have now passed their own biometric statutes or expanded existing laws to include biometric identifiers. These five states, however, either do not address the private right of action or expressly allow enforcement by the state attorneys general. Other states are also in the process of proposing their own state-specific biometric privacy statutes.

VIII YEAR IN REVIEW

In the US, it was the states that led the charge with respect to new regulations impacting the fintech industry this past year. New financial privacy, cybersecurity and biometric laws are adding yet another layer of regulatory patchwork issues for fintechs to navigate. In particular, the new California Consumer Privacy Act has been a significant burden on the fintech industry as entities have had to revamp their privacy policies and restructure their operations to comply with California consumers’ new rights to access their data, have their information
erased or opt out of data sharing. Additionally, while New York City’s decision to ban cashless businesses may not have been targeted at them, fintechs operating in the state are cautioned to carefully consider how the ban might apply to various products and services. Although the OCC is committed to moving forward with issuing its new fintech bank charter, states are equally committed to fighting any such charters. Meanwhile the CSBS continued to push Vision 2020 initiatives that will hopefully lead to significant uniformity among states regarding state licensing and regulatory issues that affect fintechs.

The past year has also shown significant maturation of the fintech industry with a number of major industry developments. The announcement early in 2020 that Visa acquired Plaid (a major US fintech that has API connections with thousands of US financial institutions) for US$5.3 billion is an important reminder that while fintech start-ups often get the headlines, more established ‘legacy’ companies in financial services technology and payments are continuing to evolve, pivot and execute strategic moves to remain competitive. In addition, fintechs may find more creative ways to acquire, rather than file de novo for bank charters, as illustrated by Lending Club’s announcement in February 2020 that it is in the process of acquiring Radius Bank, a technology-focused and API-driven financial institution, illustrating that fintechs may acquire banking charters and the people, processes, procedures and regulatory expertise of financial institutions to assist in running the combined entities. Additionally, Facebook’s ambitious unveiling of the Libra Initiative invited intense US, as well as international, regulatory scrutiny while companies continue both to join and abandon the project. These are just a few of the industry developments that foreshadow more unpredictable announcements on the horizon.

IX OUTLOOK AND CONCLUSIONS

The US financial regulatory regime is incredibly complex and ever-evolving, and can pose unique challenges to fintechs that seek to operate in the US. States and the federal government are interested in promoting innovation, but are also exceedingly cautious of new challenges and risk that innovation in the financial sector poses due to the high potential for consumer harm, as well as potential impacts on entity-level and systemic risk. As the industry matures and regulators become more educated, it is hoped that clear and consistent financial regulations will emerge.

In concluding this chapter, it is important to highlight that federal financial regulators have been overwhelmingly supportive of financial innovation for several years, but there will be a presidential election in the US in November 2020 and it is quite possible that a different administration at the federal level will take a less hands-off approach. Companies that have been operating without much regulatory concern or attention could very well find themselves in a very different position a year from now. However, fintechs that have as their main focus helping businesses and consumers gain access to better financial products and services, and those that strive to create user-friendly products and services that are ‘compliant by design’ will likely continue to receive favourable regulatory treatment, provided they actively work with the numerous applicable regulators.
ISABEL AGUILAR ALONSO

*Uría Menéndez*

Isabel Aguilar Alonso joined the firm in 2008 and is a counsel. She has more than 12 years of experience advising a wide range of financial entities, including credit entities, investment services firms, payment services firms and collective investment schemes, in regulatory and financial matters.

Within the regulatory field in particular, she advises on matters such as authorisations, cross-border provision of services, marketing of products, rules of conduct and transparency, consumers and users, disciplinary proceedings, payment services, e-money and SEPA regulations. Within the financial field, her practice includes fintech projects, financing, securitisations, assignments of receivables and security packages.

WAYNE ATKINSON

*Collas Crill LLP*

A group partner at Collas Crill LLP, Wayne Atkinson works with a broad range of regulated entities and investment funds on fundraising, transaction and investment structuring, commercial contracts and mergers and acquisitions. As one of the leaders of Collas Crill’s risk and regulatory team, he also regularly advises businesses on regulatory compliance including money-laundering issues, listing rules requirements, competition law, data protection and Guernsey financial services regulation more generally.

Wayne has also built considerable expertise in assisting company boards and activist shareholders in relation to contentious general meetings and associated issues arising out of investor actions.

A regular speaker at seminars and conferences in relation to company law, regulatory and fund matters, Wayne is well known for his down-to-earth, plain-speaking approach to explaining complex legal and regulatory issues.

Prior to joining Collas Crill in 2009, Wayne trained and qualified as a corporate lawyer with Herbert Smith in London working primarily in the firm’s investment funds and regulatory team. Following this, he spent a number of years in the British Virgin Islands advising on a range of investment funds and general corporate transactions.
CARLA DO COUTO HELLU BATTILANA
TozziniFreire Advogados

Carla has over 10 years of experience representing local and international clients in corporate and regulatory matters, and assisting in diverse transactions, including mergers and acquisitions, joint ventures and corporate restructurings. She assists companies in matters related to information technology and intellectual property, with solid experience in analysing and negotiating contracts related to these areas. Carla also works in cybersecurity and personal data protection matters, assisting clients with the preparation, analysis and review of terms of use and privacy policies, review and adjustment of internal policies and documents to clients and suppliers, internal trainings, adequacy of business models and practices in view of the current privacy laws and issues related to data breach incidents. She has been coordinating the data protection compliance projects of companies from several sectors.

She is certified by and a member of the International Association of Privacy Professionals. Carla holds an LLM degree from the University of Chicago; a specialisation degree in corporate law from the International Institute of Social Sciences; a specialisation degree in corporate contracts from the Getulio Vargas Foundation; and she is a graduate of the Law School of the Pontifical Catholic University of São Paulo.

She is recommended by The Legal 500, a well-known international legal guide.

NATALIE BELL
Collas Crill

Natalie is a senior associate in our corporate, finance and funds team, advising on all aspects of Cayman corporate and commercial law including mergers and acquisitions, joint ventures and corporate reorganisations. Natalie specialises in advising investment funds, their managers and their onshore counsel on the structuring, formation, corporate governance and ongoing operational matters of Cayman and BVI investment funds. She also advises financial services clients on licensing, ongoing obligations, regulatory reporting anti-money laundering and automatic exchange of information laws. Natalie joined Collas Crill having previously worked in the investment funds and regulatory team at another leading offshore firm in both the Cayman and BVI offices. Prior to this, she worked for Travers Smith and Eversheds (now Eversheds Sutherland) in the UK.

PIERRE E BERGER
DLA Piper UK LLP

Pierre Berger is a corporate, financial services and insurance partner in the firm’s Antwerp office. He advises Belgian and foreign multinationals on all aspects of banking, funds, financial services and insurance law. Complex regulatory issues, regulatory driven strategic projects, transactions and restructurings as well as Brexit- and fintech-related assignments are his core area of practice.

Pierre was awarded the Client Choice Award 2017 and 2018 for banking in Belgium. He is also ranked as a leading individual by The Legal 500, and is highly regarded by Chambers and IFLR. Who’s Who Legal mentions him as a global fintech expert.

Pierre has a law degree from University of Antwerp and KU Leuven and a licentiate degree in business sciences from Lessius Hogeschool. He studied abroad in Amiens (France), Champaign (USA) and Berlin (Germany).
ALEXEI BONAMIN
TozziniFreire Advogados

With experience in capital markets, and banking and finance since 1996, Alexei has expertise in public offerings, international issues, structured finance, project finance, securitisation, syndicated loans, agribusiness finance, derivatives, impact investing, green finance, social finance, sustainable finance, crowdfunding, endowments, asset management, investment funds, private equity, venture capital, corporate venture, financial innovation, fintechs, payment institutions, payment schemes, instant payments, open banking, blockchain technology, the regulation of financial institutions, securities regulation, financial compliance, financial investigation, financial enforcement and financial leniency agreements.

Mr Bonamin is a certified compliance and ethics professional with the Society of Corporate Compliance and Ethics, the vice-chairman of the International Bar Association, a member of the working groups on green bonds, green finances and financial instruments, and a member of the Social Impact Investment of LAB (Financial Innovation Laboratory). He holds an LLM degree in banking and finance from the London School of Economics and Political Science and is a graduate of the Law School of the Pontifical Catholic University of São Paulo.

He is recognised in well-known legal guides such as *Chambers Latin America, Chambers Global, The Legal 500, Latin Lawyer 250, Who's Who Legal, Expert Guides, IFLR1000* and *Análise Advocacia 500*.

PATRICK BOOT
Hunton Andrews Kurth LLP

Patrick's practice focuses on fintech, digital banking and payment solutions, banking operations and financial regulatory matters.

As a member of the financial institutions corporate and regulatory practice, Patrick assists clients with a wide range of legal and regulatory matters related to payments and payment systems, digital commerce, banking and financial services, emerging technology and internet products. He also advises large banks on digital transformation, consumer marketing initiatives and strategic partnerships.

FELIPE BORGES LACERDA LOIOLA
TozziniFreire Advogados

Senior associate in the mergers and acquisitions, telecommunications, intellectual property, information technology, privacy and cybersecurity practice groups, Felipe has more than 10 years of experience representing local and international clients in corporate, contractual and regulatory matters, and participating in several transactions, including mergers and acquisitions, joint ventures and corporate restructurings in the technology, pharmaceutical and telecommunications industries. He has been coordinating the data protection compliance projects of companies from several sectors.

Felipe worked as a visiting attorney at the corporate and securities practice group of Greenberg Traurig, PA from 2017 to 2018, and has been a member of the New York State Bar since 2019. He is also a former member of Kirkland & Ellis Corporate Lab Clinic and a former volunteer for the International Refugee Assistance Project chapter at the University of Chicago Law School.
Lacerda holds an LLM degree from the University of Chicago Law School and is a graduate of the Law School of the University of São Paulo.

SANDY BRUMBERG

Loyens & Loef Luxembourg Sàrl

Sandy has been a professional support lawyer in the banking and finance practice group since 2015. Her practice focuses on advising supervised entities (credit institutions, investment firms, investment funds, insurance undertakings) on EU and Luxembourg legal or regulatory developments that may have an impact on their activities.

ROMAN BUZKO

Buzko Legal

Roman Buzko leads the fintech practice of the firm. He also works on matters related to intellectual property and investments. Before launching the firm, Roman worked in international law firms. In addition to his Russian law degree, he holds a business degree from Rotterdam School of Management and a foreign scholar diploma from University of Arkansas School of Law. Roman is often invited to speak at fintech conferences and comment on fintech-related news for major Russian media outlets.

JOSÉ MIGUEL CARRACHO

Vieira de Almeida

José joined VdA in 2015. He is an associate in the banking and finance area of practice where he has been actively involved in several transactions, namely in securitisation deals and other banking and structured finance transactions.

He also has significant experience in fintech, payment services and blockchain/DLT matters, having worked in advising payment and e-money institutions as well as crowdfunding platforms.

FRANCISCA CÉSAR MACHADO

Vieira de Almeida

Francisca joined VdA in 2016. She is an associate in the banking and finance area of practice where she has been actively involved in several transactions, namely in securitisation deals and other banking and structured finance transactions.

She also has significant experience in fintech, payment services and blockchain/DLT matters, having worked in advising payment and e-money institutions as well as crowdfunding platforms.

TIAGO CORREIA MOREIRA

Vieira de Almeida

Tiago joined VdA in 2003. He is a partner in the banking and finance area of VdA where he has been actively involved in several transactions, namely in securitisation deals and other banking transactions, and he advises on the corporate restructuring of credit institutions.
He also has significant experience in fintech, payment services and blockchain/DLT matters, having worked in advising payment and e-money institutions as well as crowdfunding platforms.

He also has significant experience in aviation finance transactions, having worked with export credit agencies and the main financing entities involved therein.

ALAN DE SARAM
Collas Crill

Alan is the managing partner and heads up the corporate, finance and funds team of Collas Crill in the Cayman Islands. He advises a wide range of clients on all aspects of company and commercial law, with an emphasis on securities, investment funds, fintech, private equity structures and commercial transactions generally. His practice also includes all areas of listings, fund raising, regulatory advice, finance, security and capital markets. Alan previously worked with Fladgate and Dechert in London, and joined Collas Crill in 2004. He was made partner in 2007.

MARCELA WAKSMAN EJNISMAN
TozziniFreire Advogados

Co-head of TozziniFreire’s corporate and mergers and acquisitions practice, Marcela concentrates her work in the telecommunications and technology, intellectual property, privacy and entertainment industries. She has advised clients on numerous transactions, including mergers and acquisitions, joint ventures and corporate restructurings. Marcela uses her thorough knowledge of the technology and telecommunications sectors to assist clients with both regulatory and business issues. She also has extensive expertise in the defence and registration of trademarks, patents, utility models and industrial designs. Marcela has coordinated the data protection compliance projects of companies from several sectors.

Marcela is recommended by legal guides such as Chambers Global, Chambers Latin America, The Legal 500, Expert Guides, Latin Lawyer 250, Who’s Who Legal, WTR 1000 – World Trademark Review, Analise Advocacia 500 and IFLR 1000 (as a ‘notable practitioner’). She is in LACCA Approved as Latin America’s ‘leading private practitioner’ for intellectual property. She also won an award from the Euromoney Legal Media Group Americas Women in Business Law Awards 2016 for ‘best lawyer in intellectual property in Latin America’.

Marcela holds an LLM degree from Cornell University and is a graduate of the Law School of the Pontifical Catholic University of São Paulo.

DENİZ ERKAN
SRP-Legal

Erkan mainly deals with commercial law, corporate law and contracts law at SRP-Legal.

Before joining SRP-Legal, Erkan provided legal services to national and multinational corporate companies, mainly in commercial and corporate matters, and participated in M&A and due diligence projects.

Additionally she took part in litigation matters relating to labour law, commercial law and enforcement law and arbitration procedures relating to commercial law.

Erkan is a member of the Istanbul Bar Association.

She has excellent command of English and Romanian.
TOMMASO FAELLI
BonelliErede

Tommaso Faelli has been a partner at BonelliErede since 2012, and was admitted to the Italian Bar in 2002. He is also admitted to practise before the Italian Supreme Court. Tommaso assists both Italian and multinational companies in contentious and non-contentious matters relating to IP, unfair competition and IT (specifically, licence and software development agreements, application management and outsourcing), e-commerce, data protection and privacy, with a specific emphasis on profiling issues and data management in technology partnerships and joint ventures based on the Internet of Things and Big Data, in addition to direct marketing, data transfer abroad and internal auditing.

Since 2005, Mr Faelli has been an adjunct professor of IP law at the Faculty of Law at the University of Como. In 2007, he obtained a PhD in commercial law – IP and competition from the University of Parma.

Tommaso is a masters lecturer in IP and cyber-risk.

MARCUS FONSECA
TozziniFreire Advogados

Associate of the capital markets and banking and finance practices, Marcus Fonseca has been working at TozziniFreire Advogados since 2011, focusing on transactions involving the financial and banking sectors. He has experience in the implementation of cross-border financing transactions, constitution of investment funds, foreign exchange aspects, constitution of guarantees in general, auditing, derivative transactions, securitisation of receivables, as well as several issues related to the Central Bank of Brazil and the Commission of Securities. Marcus is a graduate of the Law School of the Pontifical Catholic University of Paraná.

Between 2018 and 2019, Marcus worked as an international visiting attorney at Skadden, Arps, Slate, Meagher & Flom LLP in New York.

Marcus was awarded the ‘rising star’ award by IFLR in 2019. Marcus was one of three Latin American lawyers recognised for their work in major operations in the areas of financial and corporate law in 2018 by IFLR.

VICTOR CABRAL FONSECA
TozziniFreire Advogados

Innovation specialist and associate of TozziniFreire’s technology and innovation practice group, Victor is responsible for coordinating the ThinkFuture, the first innovation programme structured by a Brazilian full-service law firm. As a lawyer, he assists technology-based clients, major companies interested in open innovation and start-ups. Additionally, Victor has published several articles about technology and innovation and he is one of the authors of Direito das Startups, the first Brazilian book on the matter with completely original content.
He is a guest professor on the law in start-ups at the Teaching and Research Institute (Insper-SP); a coordinator of the open innovation course at Future Law; a founding member of the committee for studies on legislation in creative entrepreneurship and start-ups of the Brazilian Bar Association, Pinheiros, São Paulo section; and a mentor on the Law Without Walls programme at University of Miami. Fonseca holds a master’s degree in business law, economics and social development from the Getulio Vargas Foundation; a certificate in exponential innovation from Singularity University; and is a graduate of the Ribeirão Preto Law School at the University of São Paulo.

ERIN FONTE

*Hunton Andrews Kurth LLP*

Erin’s practice focuses largely on four areas: fintech, traditional and emerging payments (including mobile), banking operations and regulatory, and privacy and data security.

Erin is co-chair of the firm’s financial institutions corporate and regulatory practice. She assists clients with a broad range of legal and regulatory matters related to payments and payment systems, digital commerce, banking and financial services, technology and internet products, privacy and data protection laws, and general corporate matters.

Erin regularly advises financial institutions and alternative payment providers regarding mobile banking, mobile payments, and mobile wallet products and services. She has been involved in the creation of new payment networks and has worked extensively on emerging products, services and network operating rules related to mobile payment systems.

THOMAS A FRICK

*Niederer Kraft Frey*

A partner at Niederer Kraft Frey, Dr Thomas A Frick holds degrees in Swiss and European law and general history and is admitted to the Swiss Bar. For over 20 years he has advised banks, securities traders, other financial intermediaries and start-ups on various legal and regulatory issues. He advises numerous fintech and other finance projects (ICOs, STOs, crypto-brokers, crowd-lending, asset management, crypto-fund projects, exchange projects, payment systems and others) and is actively involved both as a board member in banks and as a business angel in start-up companies. He frequently gives presentations on Swiss fintech regulations, and is a regular publisher on the subject and a lecturer on banking and finance law in Zurich University’s LLM programme.

CONCEIÇÃO GAMITO

*Vieira de Almeida*

Conceição heads the indirect tax team at Vieira de Almeida (VdA), advising clients on all VAT, customs and excise duty matters and representing them before the tax authorities and tax courts. Conceição also advises clients dealing with indirect tax issues in foreign jurisdictions including Angola, Cape Verde, Congo, Democratic Republic of Congo, East Timor, Gabon and Mozambique.
Conceição is a certified tax arbitrator and the Portuguese correspondent for the online publication VAT in Europe (IBFD). She is the author of several publications, including VAT and Digital Economy, Digital Economy Taxation: The Quest for a Perfect Solution, VAT on Early Termination Payments, Bitcoins & VAT, VAT on the Transfer as a Going Concern and the Portuguese chapter of the European VAT Handbook. She is also an expert trainer at the International VAT Expert Academy and at VAT Forum's International School on Indirect Taxation. She is a member of the Portuguese Bar Association, and a partner of VAT Forum, the International VAT Association and the GLCA – Global Legal Customs Association.

ÁLVARO GARRIDO MESA
Loyens & Loeff Luxembourg Sàrl
Álvaro is a member of the banking and finance department of Loyens & Loeff Luxembourg.

He represents leading investment firms, commercial banks, payment institutions, electronic money institutions and public and private companies in domestic and cross-border finance transactions, including acquisition financing, structured finance and financial regulatory matters.

He has a particular focus on financial technologies, and advises start-ups, financial institutions and investors on financing, licensing, and regulatory requirements.

He is a core member of the firm-wide fintech team, start-up team and the region team in Latin America.

Before joining Loyens & Loeff, Álvaro acquired in-house corporate experience at an S&P 500 industrial group listed on the NY Stock Exchange.

Álvaro is a member of the Luxembourg Bar and the Madrid Bar.

CARLETON GOSS
Hunton Andrews Kurth LLP
Carl leverages his experience as a lawyer with the Office of the Comptroller of the Currency to resolve financial institutions’ most complex regulatory and enforcement matters. He also counsels financial institutions on mergers and acquisitions and securities offerings.

Carl’s close collaboration with seasoned bank examiners on the supervision of problem institutions assigned to the OCC’s Special Supervision unit, as well as his role with multiple rulemakings under the Dodd-Frank Act, give him a unique, insider’s perspective on bank regulatory compliance, supervision, enforcement and public policy. Coupled with his investigative and enforcement experience acquired representing financial institutions before the CFPB, OCC, FinCEN, Federal Reserve, the FDIC and others while serving in the Financial Institutions group of a Washington, DC law firm, and corporate experience in mergers and acquisition and securities offerings, Carl is uniquely qualified to advise financial institutions on virtually all aspects of their operations.
SUHAIB ADLI HAMMAD

Hammad and Al-Mehdar

Suhaib A Hammad joined the law firm of Hammad and Al-Mehdar in 2011. He earned his LLB from the International Islamic University in Malaysia in 2008. After working for nearly a year in the interim, he then obtained an LLM from the University of Miami in 2010, specialising in international business law. Suhaib has extensive legal experience in the United States, Malaysia and Saudi Arabia. He is fluent in Arabic and English, and speaks basic Bahasa Melayu as well.

As a partner at Hammad and Al-Mehdar, Suhaib leads the commercial and intellectual property practice, focusing on ICT, TMT and life sciences. In addition, Suhaib was placed on secondment with the corporate and commercial team at Simmons & Simmons in their Dubai and London offices, and has worked on leading cross-border transactions. His experience includes advising international companies on Saudi regulations in relation to formation and operation. Suhaib was awarded a Client Choice award for 2019 in Saudi Arabia by Lexology. The firm was recognised as the best mergers and acquisitions law firm for 2017 and 2018 by the IFN law awards, and received an honourable mention as a Tier 1 firm in The Legal 500 2017 for banking and finance transactions.

TAKANE HORI

Mori Hamada & Matsumoto

Takane Hori focuses on IT and regulated transactions, with a special focus on payment services.

She was previously seconded to the Planning Division of the Planning and Coordination Bureau of the Financial Services Agency (2008–2010), and served as a member of the Financial System Council (Working Group on Advancements in Payment and Other Related Services) at the FSA (2014–2015).

She is the director of Fintech Association Japan, Japan’s largest fintech community.

EDDIE HSUUNG

Lee and Li, Attorneys-at-Law

Eddie Hsiung is an associate partner at Lee and Li, Attorneys-at-Law. He is licensed to practise law in Taiwan and New York, and is also a CPA in Washington State, the United States. His practice focuses on securities, M&A, banking, finance, asset and fund management, cross-border investments, general corporate and commercial, fintech, start-ups, etc. He regularly advises leading banks, securities firms, payment and credit cards and other financial services companies on transactional, licensing and regulatory and compliance matters, as well as internal investigation. He is familiar with legal issues regarding the application of new technologies such as fintech (e-payment, digital financial services, regulatory sandboxes) and blockchain (ICOs, cryptocurrencies, platform operators) and AI, and is often invited to participate in public hearings, seminars and panel discussions in these areas.

Eddie Hsiung received his LLB degree from National Taiwan University and holds two LLM degrees from National Taiwan University and Columbia Law School.
TAKAHIRO IIJIMA
*Mori Hamada & Matsumoto*

The principal practice areas of Takahiro Iijima are financial regulation, M&A and tax. He advises a large number of start-up companies, financial institutions and funds. Takahiro Iijima was educated at the University of Tokyo. He is a lecturer at the University of Tokyo Graduate School for Law and Politics and is currently studying at Harvard Law School (until May 2020).

SHANTHI KANDIAH
*SK Chambers*

Shanthi Kandiah is the head of SK Chambers, legal and regulatory advisers, specialising in competition law, telco regulations, data protection and cybersecurity. Her competition law practice covers antitrust litigation, cartels and sectoral competition regimes, including merger control. She regularly advises many corporations in sectors such as media and telecommunications, aviation, FMCG, construction, pharmaceuticals and other service industries covering issues ranging from competitor collaborations, cartels, pricing and rebate policies, and compliance. More recently, SK Chambers acted as coordinating counsel in the largest enforcement action to date by the Malaysia Competition Commission involving fines exceeding 200 million ringgit. On mergers, recent assignments include serving as local counsel on a multi-jurisdiction merger transaction led by a magic circle firm. She has also successfully advised on antitrust approval for acquisitions in the communications and multimedia sector. Shanthi has a masters in law from King’s College London. She holds a postgraduate-diploma in competition economics, also from King’s College London.

SARAH KENSHALL
*Burges Salmon LLP*

Sarah leads Burges Salmon’s cross-departmental fintech practice and is a director in the firm's technology and communications team. She has been involved in advising on evolving technologies for over 15 years, including work on high-profile transformational project procurements, structuring business models for commercialising new technologies, advising on commercial delivery and providing practical risk analysis and guidance.

Sarah’s team supports fintech companies with their establishment, expansion, commercial contracts, fundraising and M&A, and sponsored the 2018/2019 Tech Nation’s new fintech growth programme and the Go: Tech Awards (AI category) 2019. Sarah is a member of Tech UK.

JOON YOUNG KIM
*Kim & Chang*

Joon Young Kim is a senior attorney at Kim & Chang. His practice focuses on e-finance and fintech, insurance, non-bank financial companies, corporate governance, mergers and acquisitions and foreign direct investment.
Mr Kim regularly advises financial industry clients on regulatory, governance, and corporate law-related matters. He has also successfully advised clients in disputes and in litigation, as well as in responding to inquiries from or investigations by government and regulatory authorities.

He also regularly advises clients on legal issues relating to the latest innovations, such as blockchain technology, cryptocurrencies and cloud computing.

Mr Kim has been actively involved in publishing in various Korean and international journals and conducting lectures related to e-finance and fintech, blockchain technology, cryptocurrencies, insurance and corporate governance.

His expertise and experience have been recognised by industry experts. He has been named as a ‘next generation lawyer’ for two consecutive years in The Legal 500 Asia Pacific 2017 and 2018 editions.

SCOTT KIMPEL
Hunton Andrews Kurth LLP
Scott brings in-depth knowledge of SEC policies, procedures and enforcement philosophy to each representation.

Scott regularly advises clients across a broad sector of the economy facing sensitive reporting, compliance and enforcement matters before the Securities and Exchange Commission and other capital markets regulators. His practice encompasses a wide range of matters involving the securities laws, mergers and acquisitions, corporate governance, regulatory enforcement, administrative law and public policy. Scott also leads the firm’s working group on blockchain and distributed ledger technology.

MARISKA KOOL
Loyens & Loeff NV
Mariska Kool is a member of the litigation and risk management practice group. She specialises in advising on and litigating cases concerning IT contracts and IT disputes. Mariska has gained broad experience in negotiating contracts in the areas of outsourcing, cloud, software implementation, software and hardware maintenance (including medical equipment) and software licences. She also advises on and litigates cases involving commercial contracts (including franchise and agency agreements), liability issues, intellectual property rights (including copyrights) as well as cases concerning online reputation and unlawful publications (e-reputation, the right to be forgotten).

JENS H KUNZ
Noerr LLP
Dr Jens H Kunz is a partner in Noerr’s Frankfurt office and co-head of Noerr’s financial services regulation group. He advises national and international banks, financial services providers, payment institutions, funds initiators, asset management companies, fintechs and other companies affected by financial regulatory law on all matters relating to financial supervision, including investment and money laundering law. Apart from ongoing advice on current regulatory challenges and digitalisation projects, his practice also focuses on assisting clients with the financial regulatory aspects of transactions in the fields of funds, M&A and capital markets.
DILMUN LEACH
_Collas Crill LLP_

Dilmun Leach, group partner at Collas Crill LLP, is a funds, corporate and regulatory lawyer based in Jersey.

His funds practice includes acting on the launch of investment funds and their satellite vehicles, including co-investment and carry vehicles, advising on the Jersey AIFMD regime, and the establishment and licensing of Jersey managers. Dilmun has experience of working with fund managers investing in a variety of asset classes including debt and CLOs, private equity, real estate, infrastructure, oil and gas and virtual currencies.

Dilmun's corporate practice includes mergers and acquisitions, initial public offerings, schemes of arrangement, establishing investment vehicles to acquire a range of assets including infrastructure and real estate, and group restructurings.

His regulatory practice includes advising on marketing funds and other financial products into Jersey, change of control advice and applications to the Jersey regulator, and the launch of innovative new products including crowdfunding platforms, debt issuance vehicles and products involving virtual currencies and tokens.

Dilmun is actively involved in the Jersey finance industry, including responding to industry consultations, for example on LLCs and the Jersey private fund regime. He is a committee member of the Jersey Funds Association, a member of a working group reviewing the Jersey limited partnership law and a member of the Jersey Association of Directors.

JUNG MIN LEE
_Kim & Chang_

Jung Min Lee is a senior attorney at Kim & Chang, who specialises in finance. He primarily provides legal advice on banking regulations, finance IT, electronic banking and personal and financial information protection. Mr Lee's clients include Korean and global financial companies, Korean and global portal and platform service providers, e-commerce and payment service providers and IT service providers.

Since joining the firm in 2008, Mr Lee has advised clients on various legal, administrative, and technical regulations related to electronic banking and on the management and protection of financial transaction information. Mr Lee is also licensed to practise as a public accountant and registered as a CPA.

JUAN ENRIQUE LIZARDI BECERRA
_Hogan Lovells_

Juan Enrique Lizardi Becerra, one of the firm’s attorneys, concentrates on mergers and acquisitions, banking and corporate financing as well as financial regulatory advice. He obtained his JD degree from the Universidad Panamericana in 2016 and is currently studying for a master's degree at the same university.

LETICIA LÓPEZ-LAPUENTE
_Uría Menéndez_

Leticia López-Lapuente joined Uría Menéndez in 2004 and has been a partner of the firm since 2019. She heads the data protection and e-commerce area of the firm.
She has more than 14 years of experience advising companies in the technology sector, also advising financial and industrial companies on matters specifically related to technology and the protection of personal data.

She provides advice on commercial and regulatory aspects, including the preparation and negotiation of contracts (such as outsourcing, cloud computing and digitalisation), advice on the protection of personal data and privacy including defence in proceedings before the Spanish Data Protection Agency, cybersecurity, mergers and acquisitions with technological components, consumer law and e-commerce, use of biometric technologies, artificial intelligence, Big Data, public procurement law and representation before public administrations.

**MARIJE LOUISSE**  
*Loyens & Loeff NV*

Marije Louise, attorney at law, has been a member of the banking and finance practice group since 2010. She specialises in the laws and regulations regarding supervision of financial undertakings and financial markets with a special focus on fintech. Marije frequently publishes on financial regulatory topics in professional journals. A list of her publications is available upon request. In the last half of 2016, she was based in Loyens & Loeff’s Luxembourg office. Marije is a PhD student at the Radboud University of Nijmegen.

**AOIFE MADDEN**  
*Collas Crill*

Aoife is an associate in the corporate, finance and funds team in the Cayman Islands. She advises on all aspects of commercial and company law, in particular on matters related to investment funds, fintech, banking and corporate finance, securities and commercial transactions. Aoife regularly advises on all aspects of investment fund structuring, both hedge and private equity funds, including the launch, all regulatory elements, ongoing operations, restructuring and winding down. Prior to joining Collas Crill, Aoife practised with another leading offshore firm in the Cayman Islands as well as with McCann FitzGerald in Dublin.

**DAWN MAJOR**  
*Collas Crill*

Dawn joined Collas Crill as an articled clerk in September 2019. She is currently undertaking her first seat within the corporate, finance and funds team. She obtained a Bachelor of Laws with honours from the University of Liverpool in 2016 and successfully completed the postgraduate professional practice course with a distinction in 2018 from the Truman Bodden Law School. Prior to joining Collas Crill, Dawn was a paralegal for the Cayman Islands Monetary Authority. Her time and experience there exposed her to a wide array of financial services regulatory matters.
GARETH MALNA

Burges Salmon LLP

Gareth is an associate in Burges Salmon's funds and financial regulation team, and specialises in financial services regulation. He coordinates the financial services regulatory aspects of the firm's fintech practice, with a primary focus on payment services, crowdfunding, blockchain solutions and the implementation of RegTech solutions at regulator level.

Gareth also has expertise in the establishment, structuring, operation and winding up of UK regulated fund structures, such as OEICs, authorised unit trusts and authorised contractual schemes.

He is also the lead contact on the financial services regulatory aspects of the fintech sector and has been heavily involved with a number of policy initiatives in this sector with the FCA, Bank of England and Treasury, including a digital regulatory reporting pilot project.

His fintech clients include payment institutions and acquirers, neobanks, crowdfunding platforms and investment funds that offer tokenisation. He also advises authorised fund managers including host ACDs, investment managers and other regulated product providers.

He is the co-author of the UK chapter in The International Comparative Guide to Public Investment Funds 2018 (ICLG, 2018).

BRENNA MCGEE

Hunton Andrews Kurth LLP

Brenna practices at the intersection of financial services, technology and regulation, advising fintech start-ups, banks, and alternative payment providers on operations, transactions, and regulatory and enforcement matters.

Brenna leverages her know-how to advise banks, credit unions, fintech companies, retailers and other financial services providers on a broad range of matters related to payments, technology, virtual currencies, privacy, the blockchain, smart contracts and other innovative financial products. She frequently advises fintech companies, money transmitters and alternative payment providers on regulatory and compliance matters, with particular focus on product design, the permissibility and structure of new activities, and the applicability of federal MSB registration and state money transmission licensing requirements. She assists banks and other financial institution clients with a variety of regulatory and corporate matters, including the preparation of regulatory applications and notices; implementing digital strategies, mobile banking and other innovative financial products; and drafting and negotiating technology, outsourcing and vendor contracts. Brenna also advises retailers regarding mobile payments, digital commerce, mobile wallets, prepaid card programmes, stored value products, and privacy and data security matters.

HELENA CORREIA MENDONÇA

Vieira de Almeida

Helena joined VdA in 2007 and is currently a principal consultant integrated in the ICT practice area.
She has worked in different matters concerning information and communication technology, emerging technologies (AI, robotics, blockchain/DLT), copyright and neighbouring rights, cybersecurity and aerospace/satellites and drones-related matters. She also advises on the implementation of e-commerce platforms, digital signatures and websites. She has been involved in major operations in the technology field, including in outsourcing projects for major banks, cooperation and technology transfer projects, set-up of media services and online platforms, as well as on the drafting of laws on electronic commerce, digital signatures, protection of software and cybercrime.

She also has experience in fintech, advising on mobile payments, payment services and e-money, and provides advice on contracts with suppliers, acquirers, contracts with final users, setup of virtual wallets, among others. She has also been involved in setting up payment providers and in the analysis of legal issues relating to Bitcoin and virtual currencies in general.

IAN MONTGOMERY

Collas Crill

Ian is managing partner of the Collas Crill BVI office. He advises financial institutions, public and private businesses, individuals and funds on all aspects of corporate, commercial and finance law. His areas of expertise include mergers and acquisitions, joint ventures, private equity, debt and equity financing, public listings, security arrangements, tax efficient investment structures, corporate restructurings and reorganisations, takeovers, commercial contracts and corporate and commercial aspects of shareholder and contractual disputes.

He has significant experience advising on cross-border transactions in the real estate, financial services, energy and technology sectors, with a particular focus on transactions involving the Middle East and North Africa.

Prior to joining Collas Crill, Ian worked for Mourant Ozannes in Jersey. He has also worked for Harney Westwood & Riegels in the BVI and Pinsent Masons in London.

Ian qualified as a solicitor in Scotland in 2008 (currently non-practising), and was admitted as a solicitor in England and Wales in 2013 and the British Virgin Islands in 2014.

Ian is a member of the Law Society of England and Wales, the Law Society of Scotland and the Bar Association in the BVI.

Ian studied law at the University of Edinburgh.

He acted as BVI counsel to Extell Development Company on a $530 million loan package to facilitate the purchase and development of Brooklyn Point, currently the tallest residential tower under construction in Brooklyn, New York; as BVI counsel to Britain’s fourth largest mobile group, Three UK, on its £300 million acquisition of Transvision Investments Limited; and as BVI and Jersey counsel to a global property development and investment company on the £300 million sale of a landmark property in London.

ANNE-MARIE NICOLAS

Loyens & Loeff Luxembourg Sàrl

Anne-Marie Nicolas, attorney at law, is a partner in the banking and finance practice group. She specialises in banking and finance law and acts for banks, financial institutions, corporates and investors in various types of cross-border finance transactions, including acquisition financing, asset financings, structured finance and debt restructuring. She also advises on regulatory, insolvency and corporate governance matters.
About the Authors

Before joining Loyens & Loeff Luxembourg, Anne-Marie worked, among others, at the Luxembourg office of a major global law firm for 10 years, and headed the EMEA and India corporate and finance legal practice of an S&P 500 industrial group listed on the NY Stock Exchange.

Anne-Marie is a member of the Luxembourg Directors Association, the Luxembourg Bankers’ Association and the Luxembourg Banking Lawyers Association, and is an active member of several working groups related to the financial services industry. She has published a number of articles on finance and corporate governance-related issues. Anne-Marie is also a founding and board member of the ThinkBlockTank, an EU blockchain association.

Anne-Marie is admitted to the Luxembourg Bar and to the New York Bar. She is ranked as a Band 1 lawyer based on Chambers and Partners FinTech 2019 rankings.

ATSUSHI OKADA
*Mori Hamada & Matsumoto*

The principal practice areas of Atsushi Okada are information technology, intellectual property, data protection, cybersecurity, payment services, and electronic money. He advises on all types of domestic and cross-border transactions related to fund transfers, credit cards, prepaid cards, and mobile payment industries. Atsushi Okada was educated at the University of Tokyo and Harvard Law School. He serves as a member of the study group (and the chair of a working group) on AI and data contract guidelines for the Japanese government (METI).

FEDERICO DE NORIEGA OLEA
*Hogan Lovells*

Federico de Noriega Olea, a partner in the Mexico City office, focuses his practice on banking and finance, and financial institutions. He was a foreign associate at a global law firm’s New York office in 2007 and 2008, after which he rejoined Barrera, Siqueiros y Torres Landa (now Hogan Lovells BSTL). He was given an award for academic excellence by the Universidad Iberoamericana for scoring the highest GPA of his graduating class. He obtained an LLM degree from Harvard Law School in 2007. Chambers and Partners has ranked him for several years in the banking and finance, and mergers and acquisitions sections.

CIGDEM AYOZGER ONGUN
*SRP-Legal*

Dr Cigdem Ayozger Ongun has extensive experience in the technology, media and communication (TMC), financial technology and e-commerce markets in Turkey and also in corporate law, competition law and data protection and privacy law.

Dr Ayozger Ongun is the founder and the managing director of SRP-Legal in Istanbul Turkey. Before SRP-Legal, she spent over 10 years working for Turkcell Group. She worked as the Chief Legal & Regulation Strategies Officer of Turkcell Superonline for two years and prior to this duty, as the Head of Group Regulation Policies of Turkcell Group for eight years, respectively. She has provided legal and regulatory strategy consultancy in various matters and is experienced in the preparation of all kinds of draft regulations, licensing and regulatory compliance.
At SRP-Legal, Dr Ayozger Ongun has been providing not only legal services in her experience areas of law but also consulting in compliance and regulation strategy to sector leaders, and local and multinational companies.

Dr Ayozger Ongun obtained her PhD degree in law on data protection and privacy from Istanbul University and her LLM degree in competition law from Istanbul University and the London School of Economics.

Dr Ayozger Ongun is also a lecturer at Istanbul Technical University and Bahcesehir University Istanbul Blockchain and Innovation Center (BlockchainIST Center), which is the first university blockchain centre in Turkey. Furthermore, Dr Ayozger Ongun is currently mentoring at Endeavour Turkey, at the Advisory Board Member of the FintechTime Magazine and is a member of Turkish Industry and Businessmen Association (TUSİAD), Turkish Informatics Industry Association (TUBİSAD), Turkey Informatics Foundation (TBV) and Blockchain Turkey Platform (BCTR).

She is the author of the book *Personal Data Protection* (second edition). She wrote the data protection law section in the book *Prof. Dr. Huseyin Hatemi’s 80th Anniversary Gift*. She is the co-author of the ‘FinTech Players’ Competition with the Banks’ section in the book *Applied Competition Law Seminars*.

**STEFAN PAULMAYER**

*CMS Reich-Rohrwig Hainz Rechtsanwälte GmbH*

Stefan Paulmayer is a partner in the Vienna office of CMS and an attorney-at-law for banking and finance, specialising in financing transactions, asset-backed financing (securitisation), restructuring and insolvency law, derivative transactions, (banking) supervisory law and capital markets law. He has often worked at the interface between capital markets and regulatory law as well as corporate law in large capital market deals, and he regularly advises domestic and international clients in (real estate) financing transactions. Stefan advises issuers of classical capital market instruments such as shares and bonds as well as fintechs on their initial token offerings based on blockchain technology. As a result of his previous work at the global consulting firm PwC, he has a very pragmatic approach to business that clients appreciate. Stefan Paulmayer is repeatedly mentioned as a leading lawyer in the field of banking and finance, by *JUVE* and *IFRL1000* (‘leading lawyer’ and ‘rising star’ 2017 to 2020), among others.

**PEPIJN PINKSE**

*Loyens & Loeff NV*

Pepijn Pinkse is a tax lawyer at the corporate tax services practice of Loyens & Loeff. He advises Dutch and foreign listed multinationals, as well as large privately owned companies, on corporate income tax, mergers and acquisitions, reorganisations and IPOs. In the case of privately owned companies, he is also involved in advising shareholders.

He is a member of the fintech team and regularly advises clients across a range of financial technology fields, including payments, identity and security and data analytics. He also has a focus on initial coin offerings, cryptocurrencies and distributed ledger technology) in the broad sense.

Pepijn is a member of the Dutch Association of Tax Advisers.
FILIZ PIYAL
SRP-Legal
Ms Piyal, mainly deals with trade, e-commerce, data protection, privacy, technology and contracts at SRP-Legal. Prior to working with SRP-Legal, Ms Piyal worked as a lawyer in leading international and local law firms in Istanbul. She focused on helping clients in a wide range of legal areas including cross-border investments, international business transactions, acquisitions, finance transactions and regulatory compliance.

Filiz has experience clients in financial services, food and beverages, transportation, technology, manufacturing, retail, energy for cross-border acquisitions, international joint ventures corporate, and commercial activities and transactions including corporate maintenance work and contract drafting. She has acted for sellers, strategic buyers and PE clients in M&A projects and has substantial experience in capital venture investments.

She is a member of the Istanbul Bar Association and has a strong command of English and holds a level 2 capital markets licence.

WENDY PRONK
Loyens & Loeff NV
Wendy Pronk, attorney at law, is a member of the banking and finance practice group. She specialises in the laws and regulations regarding supervision of financial undertakings and financial markets. She has experience in advising on initiatives evolving around blockchain and fintech.

In 2017, Wendy was seconded to a Dutch credit offeror, where she focused on the rules regarding the offering of mortgage credit. In the first half of 2018, she was based in Loyens & Loeff’s Luxembourg office.

Wendy lectures frequently on financial regulatory topics. She is also a member of the Dutch Financial Law Association.

PETER REEVES
Gilbert + Tobin
Peter Reeves is a partner in Gilbert + Tobin’s corporate advisory group and is an expert and market-leading practitioner in financial services regulation and funds management. He leads the financial services and fintech practices at G+T. Peter advises domestic and offshore corporates, financial institutions, funds, managers and other market participants in relation to establishing, structuring and operating financial services sector businesses in Australia. He also advises across a range of issues relevant to the fintech and digital sectors, including platform structuring and establishment, payment solutions, blockchain solutions and global cryptoasset strategies. Chambers 2020 ranks Peter in Band 1 for fintech.

GIUSEPPE RUMI
BonelliErede
Giuseppe Rumi has been a partner at BonelliErede since 2007. His practice focuses on banking and financial law, with particular emphasis on regulatory issues. Mr Rumi regularly provides cutting-edge advice to major international and local banks, investment firms and asset management companies. He assists clients on authorisations, inspections and insolvency
proceedings; reviews of prudential architecture, corporate governance and internal controls systems; and compliance and anti-money laundering issues. He also provides assistance across the entire fintech spectrum and assists financial institutions, global technology and telecoms companies, investors and start-ups on the interplay between developments in the fields of technology, data exploitation, cybersecurity and financial regulation.

Since 2006, Mr Rumi has been involved in some of the most important mergers and acquisitions in the Italian banking industry and has specific experience in advising international companies interested in working in Italian regulated sectors. He assisted on wide governance reforms and internal audit investigations of credit institutions following changes in their corporate bodies and requests from the supervisory authorities.

In recent years, Mr Rumi has been involved in assisting, among others, the first digital credit platform with a full banking licence in opening its first branch in Italy; a leading group of insurance undertakings and insurance brokers in developing a blockchain system allowing the collection of the information and documents necessary for the issuance of large-risk policies; and an Italian financial intermediary in relation to the analysis of an innovative product that enables the purchase of credits for deferred payment through a digital solution entailing the use of points of sale.

Mr Rumi regularly sits on panels of Italian associations that deal with prudential supervision and complex and innovative financial techniques for both the banking sector and finance companies, and is in charge of the coordination of BonelliErede's outpost in Frankfurt at Hengeler Mueller’s premises.

**MARTIJN SCHOONEWILLE**

*Loyens & Loeff NV*

Martijn Schoonewille, attorney at law, is a member of the banking and finance practice group. He specialises in advising fintechs and financial institutions – including banks, investment firms, fund managers, custodians, trading platforms and insurers – on legal and financial regulatory aspects of their businesses and transactions in the Netherlands and, where relevant, the continental European markets. In addition, Martijn acts as counsel to financial institutions, investors and companies in a variety of public and private debt offerings and alternative financing structures.

He is one of the driving forces behind the Loyens & Loeff Tech Academy and has a particular interest in artificial intelligence, smart contracts and DLT uses in financial markets.

With a background in corporate and M&A, Martijn was seconded in 2008 to an investment bank. From the beginning of 2010 to the end of 2012 he was based in Loyens & Loeff’s London office.

Martijn speaks frequently on financial regulatory topics at universities and conferences. He is also a member of the Dutch Association for Financial Law.

**LAURA SMALLEY**

*Collas Crill*

Laura is an associate in the corporate, finance and funds team. She advises on all aspects of commercial and company law, including matters related to investment funds, banking and corporate finance, data protection legislation, securities and commercial transactions. Prior to joining Collas Crill, Laura practised in-house at Dixons Carphone plc’s global headquarters as well as with Eversheds (now Eversheds Sutherland) in London.
ABE T S SUNG  
*Lee and Li, Attorneys-at-Law*

Abe T S Sung is a partner at Lee and Li, Attorneys-at-Law. His main practice areas are banking, structured finance, capital market and general corporate matters. He has advised many domestic and foreign financial institutions in their financing deals as well as regulatory and compliance matters, including Citi Bank, ANZ Bank, BNP Paribas, Credit Agricole, Societe Generale, Uni Credit Bank, BBVA, Mizuho Bank, Bank of Tokyo-Mitsubishi UFJ, Bank of Taiwan, CTBC Bank, Taishin Bank and Bank SinoPac. He also helped to structure Taiwan’s milestone project financing deal for the development of Taiwan High Speed Rail, and was actively involved in several other BOT and structured financing deals, such as refuse incineration plants, power plants and urban area redevelopment. According to *Chambers Asia*’s survey, clients commend him for combining ‘commercial sense with an open mind’, and consider him ‘the first choice’ for structured finance.

Abe Sung received his LLB degree from Fu-Jen Catholic University and holds an LLM degree in international banking law from Boston University Law School.

ADRIAN ANG V-MENG  
*Allen & Gledhill LLP*

Adrian is co-head of Allen & Gledhill’s fintech practice.

Adrian has been active in the fintech sphere, contributing to policy formation and the enactment of fintech-related legislation. He has advised on a variety of fintech models including payment services such as e-wallet providers, merchant acquirers, equity and debt crowdfunding platforms, P2P lending platforms, online lending intermediary based platforms, online money transfer systems, online payment system providers, robo-advisers, initial coin offering structures, security token exchanges and digital payment token exchanges.

Adrian graduated from the University of Oxford with a BA (Hons) degree in 2002 and an MA in 2006. He was called to the Singapore Bar in June 2004 and is a non-practising solicitor of England and Wales.

Adrian is recommended as a key practitioner in several leading publications. In the area of fintech, Adrian is ranked as a Band 1 fintech practitioner in Chambers *FinTech 2020*. One source comments that he is ‘outstanding at any point in time’ and another source states that he has ‘never seen an external lawyer respond in such a fast, succinct way. His responsiveness is incredible.’ Adrian is also the only lawyer who is named as a ‘global elite thought leader’ in Asia-Pacific by *Who’s Who Legal in its Banking 2020: Fintech Analysis*. *Who’s Who Legal* also notes that he is ‘one of the stars of the international fintech market. Clients enthusiastically praise his ‘deep understanding of capital markets, the jaw-dropping speed of his responses and his affable yet professional nature’. In addition, Adrian is ‘renowned for his “unparalleled understanding of blockchain technology”’, and ‘clients across the board comment that they “have complete confidence in him”, praising his “ability to connect the dots from a both technological and legal perspective”’.  

Prior to joining Allen & Gledhill in 2011, Adrian was with the Monetary Authority of Singapore and was in legal practice in London and Singapore.
MARC VAN DE LOOVERBOSCH  
DLA Piper UK LLP

Marc Van de Looverbosch is an associate in the Antwerp office. He advises clients on all aspects of financial services regulation, structuring and litigation, with an emphasis on blockchain-related projects. Before joining DLA Piper, Marc gained substantive experience as a lawyer in the corporate finance department of another reputable international law firm, where he focused on public capital raisings and M&A work.

In addition to his work as a lawyer, Marc is currently conducting PhD research on good faith acquisition of financial assets at KU Leuven (Belgium). He has published several articles on corporate and financial law and blockchain technology, including the first article in Belgian literature on crypto-securities.

Marc has law degrees from KU Leuven and the University of Antwerp.

FEDERICO VEZZANI  
BonelliErede

Federico Vezzani has been a partner at BonelliErede since 2015. His practice focuses on banking and insurance regulations, with particular focus on supervisory and regulatory matters relating to banks, insurance companies and Italian and international financial intermediaries. He advises both financial institutions and non-regulated firms on the Italian and EU financial regulatory aspects of a broad range of matters and projects, including capital strengthening measures through the issuance of equity, hybrid, subordinate and convertible instruments, liability management transactions and funding of debt instruments, plain vanilla and structured, through standalone issuance of securities or in relation to domestic and international programmes.

He also has a profound knowledge of the fintech sector, continually assisting clients in the evolution of financial services deriving from technological innovation, changing customers’ expectations and empowerment and regulatory developments. Mr Vezzani also has considerable experience in equity and debt capital markets transactions, as well as in the asset management sector.

He recently advised one of the most important banks investing in fintech funds, and has been involved in assisting, among others, clients of an Italian cryptocurrency exchange platform in discussions with Consob and on the procedures to obtain judicial declaration of the bankruptcy of the company holding and managing the platform; and an Italian info-rating provider in respect of the regulatory and corporate matters arising from the setting-up of a newco, providing digital lending services including the purchase of receivables from Italian SMEs.

YU PUI HANG (HENRY YU)  
Henry Yu & Associates, in association with L & Y Law Office

Mr Yu Pui Hang (Henry Yu) is the principal partner of L & Y Law Office and Henry Yu & Associates. His areas of expertise include blockchain, commercial law, corporate and commercial transactions and foreign and cross-border investments. Mr Yu is a member of the Innotech Committee (formerly known as the Technology Committee) of the Law Society of Hong Kong, and has also been appointed as the Hon. Legal Advisor to the Hong Kong Federation of Innovation and Invention, Hon. Legal Advisor to the Hong Kong
About the Authors

International Blockchain & Financial Association, Hon. Legal Advisor to the Institute of Financial Technologies of Asia and Hong Legal Advisor to the Bitcoin Association of Hong Kong. From time to time, Henry represents the Bitcoin community at meetings with the Legislative Council Members, the HKMA and the FTSB.

ALEXANDER YAP WEI-MING

Allen & Gledhill LLP

Alexander is co-head of Allen & Gledhill’s fintech practice. He focuses on the acquisition, divestiture, provision, sharing or receipt of technology and intellectual property-related assets, data and services. Alexander is recommended by Who’s Who Legal: Banking – Fintech 2020, which notes he is ‘a highly endorsed fintech specialist who boasts extensive experience advising on a range of matters including internet banking and online trading’, with a source effusing that ‘Alexander not only possesses a sharp intellect but also the ability to convey and communicate legal intricacies in simple terms’. He is ‘identified for his “ability to negotiate outcomes for parties”, as well as his “strong skills in the tech space”’.

Alexander advises on intellectual property licensing, R&D and sponsorship arrangements, cybersecurity, collaboration agreements, outsourcing, distribution and franchising, online gaming, the cloud and ‘as-a-service’ platforms, and is a key contact for data protection and privacy compliance matters and data breach management. He is recommended for his expertise in intellectual property work by The Legal 500 Asia Pacific 2019 which notes him as ‘a key name for commercial transactions relating to intellectual property, information technology and the protection and management of data’.

NATASHA WIEDMANN

TozziniFreire Advogados

Associate of the capital markets and banking and finance practices, Natasha Wiedmann has been working at TozziniFreire Advogados since 2010. She has solid experience of administrative sanctioning proceedings held by the National Financial System’s Council of Appeals, the Brazilian Central Bank, the Brazilian Securities and Exchange Commission, the Brazilian Federal Audits Court, the Federal Public Prosecutor’s Office and other regulatory bodies.

She is also responsible for developing several consultative works on matters related to banking law and capital markets law in general, including fintechs, investment funds, financing operations and compliance.

Between September 2019 and February 2020, Natasha worked at the World Bank Group as a trainee, assisting its Legal Vice Presidency’s corporate finance practice group in Washington, DC and as a legal consultant in Brasilia.

Natasha holds an LLM degree in international and European business law from the Katholieke Universiteit Leuven.

SAMUEL YIM

Kim & Chang

Samuel Yim is a senior foreign attorney at Kim & Chang’s e-finance and fintech practice, where he focuses on blockchain and cryptocurrency matters. He regularly represents token sellers, cryptocurrency exchanges, ventures, hedge and private equity funds and their portfolio companies, token marketers and broker-dealers, funds interested in trading digital assets,
global investment banks, financial institutions and asset managers, and others in the space. He has advised foreign and domestic clients on major industry, defining matters such as, among others, initial coin offerings (ICOs) and reverse ICOs, token private placements, the establishment or acquisition of cryptocurrency exchanges, cryptocurrency arbitrage, and the establishment of cryptocurrency not-for-profit foundations.

Prior to joining Kim & Chang, Mr Yim worked at Allen & Overy LLP and served in the US Army. Mr Yim received a BS from the United States Military Academy (West Point) and a JD/MA from Georgetown University Law Center and the Paul H Nitze School of Advanced International Studies, Johns Hopkins University. He received the Fulbright Fellowship and studied at Yonsei University in Seoul, Korea. Mr Yim was also an adjunct professor at Yonsei University Law School and was a term member on the Council on Foreign Relations. He is admitted to the New York Bar.
Appendix 2

CONTRIBUTORS’ CONTACT DETAILS

ALLEN & GLEDHILL LLP
One Marina Boulevard #28-00
Singapore 018989
Tel: +65 6890 7188
Fax: +65 6327 3800
adrian.ang@allenandgledhill.com
alexander.yap@allenandgledhill.com
www.allenandgledhill.com

BONELLIEREDE
1 Via Barozzi
20122 Milan
Italy
Tel: +39 2 77 11 31
Fax: +39 2 77 11 32 60
giuseppe.rumi@belex.com
federico.vezzani@belex.com
tommaso.faelli@belex.com
www.belex.com

BURGES SALMON LLP
One Glass Wharf
Bristol BS2 0ZX
United Kingdom
Tel: +44 117 939 2000
gareth.malta@burges-salmon.com
sarah.kenshall@burges-salmon.com
www.burges-salmon.com

BUZKO LEGAL
33/8 Kuibysheva, 3rd floor
Saint Petersburg 197046
Russia
Tel: +7 499 112 33 47
roman.buzko@buzko.legal
www.buzko.legal

COLLAS CRILL
125 Main Street
PO Box 144
Road Town
Tortola
British Virgin Islands
Tel: +1 284 852 6316
ian.montgomery@collascrill.com

Gletney Court
PO Box 140
Gletney Esplanade
St Peter Port
Guernsey GY1 4EW
Tel: +44 148 173 4281
wayne.atkinson@collascrill.com

Gaspé House
66-72 Esplanade
St Helier
Jersey JE1 4XD
Tel: +44 1534 601745
dilmun.leach@collascrill.com
Contributors' Contact Details

Floor 2, Willow House
Cricket Square
PO Box 709
Grand Cayman KY1-1107
Cayman Islands
Tel: +1 345 949 4544
alan.desaram@collascrill.com
natalie.bell@collascrill.com
aoife.madden@collascrill.com
laura.smalley@collascrill.com
dawn.major@collascrill.com

www.collascrill.com

Hammad and Al-Mehdar
Level 12, Office 1209
King Road, King Road Tower
Jeddah
Saudi Arabia
Tel: 920004626
Fax: +966 (0)126069190
suhaib.hammad@hmco.com.sa
www.hmco.com.sa

Henry Yu & Associates, in Association with L & Y Law Office
Suite 806, 8/F Tower Two
Lippo Center, 89 Queensway
Admiralty
Hong Kong
Tel: +852 2115 9525
hyu@lylawoffice.com
www.lylawoffice.com

Hogan Lovells
Paseo de Tamarindos 150-PB
Bosques de las Lomas
Cuajimalpa de Morelos
Mexico City 05120
Mexico
Tel: +52 55 5091 0000
Fax: +52 55 5091 0123
federico.denoriega@hoganlovells.com
juan.lizardi@hoganlovells.com
www.hoganlovells.com

Gilbert + Tobin
Level 35, Tower Two
International Towers Sydney
200 Barangaroo Avenue, Barangaroo
Sydney, NSW 2000
Australia
Tel: +61 2 9263 4000
Fax: +61 2 9263 4111
www.gtlaw.com.au
HUNTON ANDREWS KURTH LLP
IBC Bank Plaza
500 West 5th St, Suite 1350
Austin TX 78701
United States
Tel: +1 512 542 5011
Fax: +1 512 542 5049
efonte@huntonak.com
skimpel@huntonak.com
cgoss@huntonak.com
pboot@huntonak.com
bmcgee@huntonak.com
huntonak.com

KIM & CHANG
39 Sajik-ro 8-gil
Jongno-gu
Seoul 03170
Korea
Tel: +82 2 3703 1114
Fax: +82 2 737 9091/9092
jungmin.lee@kimchang.com
joonyoung.kim@kimchang.com
samuel.yim@kimchang.com
www.kimchang.com

LEE AND LI, ATTORNEYS-AT-LAW
No. 555, Section 4, Zhongxiao East Road,
Xinyi District
Taipei 11072
Taiwan
Tel: +886 2 2763 8000 (2232 / 2162)
Fax: +886 2 2766 5566
abesung@leeandli.com
eddiehsiung@leeandli.com
www.leeandli.com

LOYENS & LOEFF
Loyens & Loeff Luxembourg Sàrl
18-20, rue Edward Steichen
2540 Luxembourg
Luxembourg
Tel: +352 46 62 30
Fax: +352 46 62 34
alvaro.garrido.mesa@loyensloeff.com
anne-marie.nicolas@loyensloeff.com
sandy.brumberg@loyensloeff.com

Loyens & Loeff NV
Fred. Roeskestraat 100
1076 Amsterdam
Netherlands
Tel: +31 20 578 57 85
Fax: +31 20 578 58 00
martijn.schoonewille@loyensloeff.com
wendy.pronk@loyensloeff.com
marije.louisse@loyensloeff.com
mariska.kool@loyensloeff.com
pepijn.pinkse@loyensloeff.com
www.loyensloeff.com

MORI HAMADA & MATSUMOTO
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi
Chiyoda-ku
Tokyo 100-8222
Japan
Tel: +81 3 6212 8330
Tel: +81 3 6212 8230
atsushi.okada@mhm-global.com
takane.hori@mhm-global.com
takahiro.iiijima@mhm-global.com
www.mhmjapan.com

NIEDERER KRAFT FREY
Bahnhofstrasse 53
8001 Zurich
Switzerland
Tel: +41 58 800 8000
Fax: +41 58 800 8080
thomas.a.frick@nkf.ch
www.nkf.ch

© 2020 Law Business Research Ltd
Contributors’ Contact Details

NOERR LLP
Börsenstraße 1
60313 Frankfurt
Germany
Tel: +49 69 971477218
Fax: +49 30 20942094
jens.kunz@noerr.com
www.noerr.com

SK CHAMBERS
9B Jalan Setiapuspa
Bukit Damansara
50490 Kuala Lumpur
Malaysia
Tel: +60 3 2011 6800
Fax: +60 3 2011 6801
sk@skchambers.co
www.skchambers.co

SRP-LEGAL
Maslak, Ahi Evran Caddesi 42 Maslak No: 6
A Kule Kat 27 Daire: 8
34398 Sarıyer
Turkey
Tel: +90 212 401 44 01
www.srp-legal.com

TOZZINIFREIRE ADVOGADOS
Rua Borges Lagoa 1328
São Paulo 04038-904
Brazil
Tel: +55 11 5086-5000
abonamim@tozzinifreire.com.br
mejinisman@tozzinifreire.com.br
ccouto@tozzinifreire.com.br
vfonseca@tozzinifreire.com.br
mfonseca@tozzinifreire.com.br
nwiedman@tozzinifreire.com.br
fblacerda@tozzinifreire.com.br
http://tozzinifreire.com.br

URÍA MENÉNDEZ
c/ Príncipe de Vergara, 187
Plaza de Rodrigo Uría
Madrid 28002
Spain
Tel: +34 91 586 04 00
Fax: +34 91 586 04 03
leticia.lopez-lapuente@uria.com
isabel.aguilar@uria.com
www.uria.com

VIEIRA DE ALMEIDA
Rua Dom Luis I, 28
1200-151 Lisbon
Portugal
Tel: +351 21 311 3400
Fax: +351 21 311 3406
tcm@vda.pt
hcm@vda.pt
crg@vda.pt
jmc@vda.pt
fpm@vda.pt
www.vda.pt

© 2020 Law Business Research Ltd
For more information, please contact info@thelawreviews.co.uk

THE ACQUISITION AND LEVERAGED FINANCE REVIEW
Marc Hanrahan
Milbank LLP

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW
Mark F Mendelsohn
Paul, Weiss, Rifkind, Wharton & Garrison LLP

THE ASSET MANAGEMENT REVIEW
Paul Dickson
Slaughter and May

THE ASSET TRACING AND RECOVERY REVIEW
Robert Hunter
Edmonds Marshall McMahon Ltd

THE AVIATION LAW REVIEW
Sean Gates
Gates Aviation LLP

THE BANKING LITIGATION LAW REVIEW
Christa Band
Linklaters LLP

THE BANKING REGULATION REVIEW
Jan Putnis
Slaughter and May

THE CARTELS AND LENIENCY REVIEW
John Buretta and John T erzaken
Cravath Swaine & Moore LLP and Simpson Thacher & Bartlett LLP

THE CLASS ACTIONS LAW REVIEW
Camilla Sanger
Slaughter and May

THE COMPLEX COMMERCIAL LITIGATION LAW REVIEW
Steven M Bierman
Sidley Austin LLP