ACKNOWLEDGEMENTS

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

ALLEN & GLEDHILL LLP
ALLEN & OVERY LLP
BONELLIEREDE
BURGES SALMON LLP
BUZKO & PARTNERS
COLLAS CRILL
DLA PIPER UK LLP
GILBERT + TOBIN
HOGAN LOVELLS
KIM & CHANG
LEE AND LI, ATTORNEYS-AT-LAW
LOYENS & LOEFF
McAFEE
MORI HAMADA & MATSUMOTO
NIEDERER KRAFT FREY
NOERR LLP
SHEARMAN & STERLING
SK CHAMBERS
STADLER VÖLKEL RECHTSANWÄLTE GMBH
TOZZINIFREIRE ADVOGADOS
URÍA MENÉNDEZ
VIEIRA DE ALMEIDA
CONTENTS

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

Chapter 1 IMPACT OF THE NEW INFOSEC AND EU PRIVACY REQUIREMENTS ON BANKS AND FINANCIAL INSTITUTIONS’ USE OF CLOUD COMPUTING .... 1
  Roy Kamp and Noémie Weinbaum

Chapter 2 AUSTRALIA ...................................................................................................................................... 12
  Peter Reeves

Chapter 3 AUSTRIA ........................................................................................................................................ 26
  Oliver Völkel and Bryan Hollmann

Chapter 4 BELGIUM ...................................................................................................................................... 35
  Pierre E Berger, Stéphanie Liebaert and Marc Van de Looverbosch

Chapter 5 BRAZIL ......................................................................................................................................... 49
  Alexei Bonamin, Carla do Couto Hellu Battilana, Ivan Antonio Monteiro Marques, Maria Eugenia Geve de Moraes Lacerda, Thais Helena Valente Teixeira Lima and Victor Cabral Fonseca

Chapter 6 BRITISH VIRGIN ISLANDS ........................................................................................................... 59
  Stephen Adams

Chapter 7 CAYMAN ISLANDS ....................................................................................................................... 66
  Stephen Nelson

Chapter 8 FRANCE ......................................................................................................................................... 75
  Eric Roturier

Chapter 9 GERMANY ...................................................................................................................................... 85
  Jens H Kunz
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Country</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 10</td>
<td>GUERNSEY</td>
<td>Wayne Atkinson</td>
<td>101</td>
</tr>
<tr>
<td>Chapter 11</td>
<td>ITALY</td>
<td>Giuseppe Rumi, Federico Vezzani and Tommaso Faelli</td>
<td>110</td>
</tr>
<tr>
<td>Chapter 12</td>
<td>JAPAN</td>
<td>Atsushi Okada, Takane Hori and Takahiro Iijima</td>
<td>125</td>
</tr>
<tr>
<td>Chapter 13</td>
<td>JERSEY</td>
<td>Dilmun Leach</td>
<td>138</td>
</tr>
<tr>
<td>Chapter 14</td>
<td>KOREA</td>
<td>Jung Min Lee, Joon Young Kim and Samuel Yim</td>
<td>149</td>
</tr>
<tr>
<td>Chapter 15</td>
<td>LUXEMBOURG</td>
<td>Anne-Marie Nicolas, Álvaro Garrido Mesa, Konstantinos Georgiou and Sandy Brumberg</td>
<td>163</td>
</tr>
<tr>
<td>Chapter 16</td>
<td>MALAYSIA</td>
<td>Shanthi Kandiah</td>
<td>177</td>
</tr>
<tr>
<td>Chapter 17</td>
<td>MEXICO</td>
<td>Federico de Noriega Olea and Juan Enrique Lizardi Becerra</td>
<td>188</td>
</tr>
<tr>
<td>Chapter 18</td>
<td>NETHERLANDS</td>
<td>Martijn Schooneville, Wendy Pronk, Marije Louise, Mariska Kool and Pepijn Pinkse</td>
<td>198</td>
</tr>
<tr>
<td>Chapter 19</td>
<td>PORTUGAL</td>
<td>Tiago Correia Moreira, Helena Correia Mendonça, Conceição Gamito and José Miguel Carracho</td>
<td>209</td>
</tr>
<tr>
<td>Chapter 20</td>
<td>RUSSIA</td>
<td>Roman Buzko</td>
<td>220</td>
</tr>
<tr>
<td>Chapter 21</td>
<td>SINGAPORE</td>
<td>Adrian Ang V-Meng and Alexander Yap Wei-Ming</td>
<td>231</td>
</tr>
<tr>
<td>Chapter 22</td>
<td>SPAIN</td>
<td>Leticia López-Lapuente and Isabel Aguilar Alonso</td>
<td>239</td>
</tr>
</tbody>
</table>
Chapter 23  SWITZERLAND .................................................................250
Thomas A Frick

Chapter 24  TAIWAN ........................................................................262
Abe T S Sung and Eddie Hsiung

Chapter 25  UNITED KINGDOM ...............................................................271
Gareth Malna and Sarah Kenshall

Chapter 26  UNITED STATES .................................................................283
Jordan Altman and Reena Agrawal Sahni

Appendix 1  ABOUT THE AUTHORS .....................................................293
Appendix 2  CONTRIBUTORS’ CONTACT DETAILS .................................311
This is already the second edition of *The Financial Technology Law Review*. Concerns about new developments that blockchain, big data and AI will trigger in the finance sector have not disappeared since the first edition. However, the use of IT in the finance sector is not new and many applications that would be labelled today as fintech are already quite old, at least by today’s standards. Financial market participants and their legal advisers already have considerable experience in implementing such changes. As far as improved support products are concerned, the general rules of financial regulations can be applied quite easily to new developments.

Some of the recent developments may already have seen their peak, for example, the great number of cryptocurrencies imitating bitcoin. Others, in particular stablecoins and security tokens, but also robo-advisers and the use of big data, AI and other blockchain applications, may still be at an early stage. They may have the potential to disrupt the industry, at least in some of its sectors. Again, there has been more scepticism, not only in a recent report by the Bank for International Settlements but also in management consultant studies such as ‘Blockchain’s Occam problem’, arguing that blockchain is a technology in search of a problem.

Regulators’ surprise about the sheer dynamism of these advances – both the speed of the technical developments and the speed with which such new possibilities were implemented – has ebbed and a number of countries have started to draft (or have already implemented) new laws or changes to their current laws to address fintech issues. This is particularly the case in the area of anti-money laundering rules, a prime concern not only of regulators but also of 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.

The national solutions chosen (and the speed with which regulators are willing to react by providing guidelines to market participants) varies considerably between jurisdictions. This may be a consequence of different regulatory cultures, but in addition, the existing legal systems may pose varying and unplanned obstacles to the some of the new applications. It may, for example, be difficult to transfer rights on the blockchain if the national code prescribes that rights can only be assigned in writing. Therefore, a structured collection of overviews over certain aspects of fintech law and regulation such as the present one continues to be valuable not only for the international practitioner, but also for anyone who looks 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 any of the varied issues fintech raises in the legal and regulatory field.

The emphasis of this collection 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, of the editor or of 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
April 2019
Chapter 1

IMPACT OF THE NEW INFOSEC AND EU PRIVACY REQUIREMENTS ON BANKS AND FINANCIAL INSTITUTIONS’ USE OF CLOUD COMPUTING

Roy Kamp and Noémie Weinbaum

I INTRODUCTION

Owing to the spread of digitalisation within the world of banks and financial institutions, and coupled with the fact that a good number of back office functions in banks are now being outsourced and that both banks and third-parties are major customer of cloud services providers (CSPs), the legal requirements applicable to cloud computing induce an ambiguous tension between the cloud computing guidelines issued by the European Banking Authority (EBA) and the Standard Contractual Clauses (SCCs) that are expected to be replaced now that the General Data Protection Regulation 2016/679 (GDPR) is in force. This relationship is crystallising around three main stumbling points:

a information security requirements, also referred to as technical and organisational measures (TOMs);
b subcontracting, also now known as sub-processing when the subcontracting involves the processing of personal data; and
c audit rights.

Professionals are contemplating a hide-and-seek game between the EBA and the European Commission, or rather – if we dare to say – a love-hate relationship that is detrimental to business and IT efficiency.

Let us hope that the EU Commission and the EBA find a compromise to put an end to this game by putting a term to the discrepancies existing between the Second Payment Services Directive (PSD2) and the GDPR, and ensuring that the EBA’s guidelines are realistic for CSPs by using adapted, standardised mechanisms including the Code of Conduct for Cloud Services Providers and updated SCCs that include TOMs based on the ISO 27001 standards. We hope that this chapter will contribute to the draft of a roadmap for an enlightened outcome.

1 Roy Kamp is a data protection officer and Noémie Weinbaum is an attorney at McAfee.
II TOPICS SPECIFIC TO BANKS AND OTHER FINANCIAL INSTITUTIONS

i Historical context

Banks and other financial institutions have been concerned by trust as early as the 15th century, when the letter of credit enabled globalised business. And as history repeats itself:

we are [today] living in the Renaissance era of banking and this transformation that we see is from disruptive changes across regulations, technology, and the very manner in which banking is consumed as a service. The opportunity to transform banking is now the top agenda for most nations globally, as they seek to make banking inclusive and accessible to billions.²

Privacy and infosec – as the basis for such trust – have been the core elements of banking regulations as early as 2006,³ when the Committee of European Banking Supervisors released its Guidelines on Outsourcing and disclosed a set of principles-based guidelines to provide national supervisors with an adequate degree of flexibility to take into account domestic rules and specific features of their local markets and to encourage developments in market practices.

The EBA's Guideline 8 provides that:

[all] outsourcing arrangements should be subject to a formal and comprehensive contract. The outsourcing contract should oblige the outsourcing service provider to protect confidential information.⁴

ii The French Ministerial Order of 3 November 2014 in relation to the internal control of credit institutions and investment firms subject to the supervision of the French Prudential Control Authority

These Guidelines have been translated into national regulations, specifically in France as the French Ministerial Order dated 3 November 2014 in relation to the internal control of credit institutions and investment firms subject to the supervision of the French Prudential Control Authority (the Order).⁵

The Order sets out obligations for French banks and financial institutions in relation to a bank's internal control and for the outsourcing of services qualified as 'essential' (essential outsourced services or EOSs).

These EOSs are defined as:

services or other operational tasks which are essential or important for the bank's activity and which are transferred to a third party (the 'Supplier') on a regular and lasting basis.

Essential services are defined in the Order as:

(i) banking activities; activities related to banking activities; activities directly linked to banking activities; and any other activities of such importance that any weakness or failure in the provision

⁴ id. Guideline No.8.
of these activities could have a significant effect on the bank’s ability to meet its regulatory obligations and/or to continue its business; (ii) any other activities requiring a licence from the supervisory authority; (iii) any activities having a significant impact on its risk management; and (iv) the management of risks related to these activities.

If outsourced to a supplier, any services or tasks falling within the first three categories above are automatically considered as an EOS.

The fourth category requires French banks to assess for themselves whether a given high-risk activity, if outsourced, should be qualified as an EOS. If the analysis by the relevant internal compliance department of the bank concludes that a given outsourced activity falls within the fourth category, such activity will be considered an EOS and the contract with the supplier would be required to comply with specific contractual requirements. The supplier additionally would need to undertake to:

- abide by service levels (SLAs);
- protect the integrity and confidentiality of any information processed by it (confidentiality, security and data protection clauses need to be included in the contract);
- provide contingency mechanisms in case of any serious problem or force majeure event in order to ensure the service continuity of the bank (a business continuity plan (BCP) needs to be included in the contract);
- provide regular reports on the performance of the service and on any events that might have a significant impact on the supplier’s capacity to perform the outsourced services in an efficient and compliant manner; and
- access on-site, whenever the bank deems it necessary, to audit all information and systems relating to the services, in compliance with applicable regulations governing disclosure, and allow the European Central Bank (or, in France, the Prudential Supervision and Resolution Authority, independent public supervisory authority for the banking and insurance sectors) to have access, including on-site, to information necessary to their mission in relation to understanding and inspecting the services provided under the contract.

The Order also provides for the requirement for the supplier to obtain the express written consent of the bank before making changes to the outsourced services, and before outsourcing any of such services to any third party (or fourth party) or concluding a service or subcontracting agreement with a third party concerning the outsourced services in order to ensure full compliance of said agreements to the Order.

Among other obligations are the requirement to insert a termination and an exit management clause to allow the outsourced services to be transferred to another supplier or to be reintegrated by the bank, and the more generic concern to consider the relationship as based on intuitu personae, namely, where the specific contracting party and its suppliers are material terms of the contract and cannot be changed without the customers’ consent.
In July 2018, the EBA updated the 2006 Guidelines on Outsourcing. We may assume that a heated debate will ensue between CSPs and banks and financial institutions as to which software or services will be classified as ‘material’. Each bank will, therefore, be required to notify competent authorities of the outsourcing on a case-by-case basis.

And where the CSP will strongly defend the fact that the Order provides that:

Without prejudice to the assessment of any other task, the following tasks shall not be considered as services or other essential or important operational tasks:
- the supply to the reporting enterprise of consultancy services and other services not included in the activities covered by its accreditation or authorisation, including the provision of legal advice, training of its personnel, billing services and the security of the premises and the personnel of the enterprise;
- the purchase of standard services, including services providing market information or price data feeds.

Market data and other standard services that do not require the implementation of sophisticated integration services can be argued as being de facto out of scope. The same could apply to public clouds that are not specifically tailored to a particular customer when used for general purposes and for the purposes included in the bullets above.

It is common practice for banks and financial institutions to argue that where a bug or a failure of the service likely would lead to serious impacts on the ability of the institution to comply with its obligations relating to the exercise of its activity, its financial performance or the continuity of its services and activities, such software or service should be qualified as an EOS.

Therefore, if failure of the part of the computer system deployed in the cloud is likely to undermine the continuity of the services and activities of the financial and banking institution, the use of cloud computing is also likely to be qualified as an EOS, implying stronger obligations including requirements to:

\[a\] have an exit plan agreed to in the contract and a BCP;
\[b\] share the contract with the competent authority;
\[c\] have full access to the business premises (the head office as well as any operations centre) for providing outsourced services. This access right includes the following:
  - an unrestricted right of inspection and audit by bank or appointed third party as defined in the contract, unimpeded or limited by contractual arrangements;
  - the right to agree alternative assurance level if other clients’ rights are affected;
  - third-party certification is possible; however, there is the right to request an expansion of the scope of the audit to certain systems or controls (based on reasonable and legitimate grounds);
  - the right for the customer to check that auditors have correct level of skill and knowledge to perform the audits;
  - an unrestricted contractual right for competent authority to inspect and audit services, subject to confidentiality;
  - notice of audit or access within a reasonable time period; and
  - full cooperation with onsite visit;

---

6 Footnote 23.
7 Article 10 of the Order opt. cit. 3.
Infosec and EU Privacy Requirements

d) set confidentiality and security standards for the protection of data (integrity and traceability of data and critical systems), with standards monitored on an ongoing basis;
e) no prohibition on outsourcing outside the EEA, but noting issues arising for effective supervision;
f) inform the bank of change to any subcontractors sufficiently in advance to allow the bank to make an assessment on new subcontractors;
g) the right to terminate where a change of subcontractor results in an adverse effect on services; and
h) review and monitor services on an ongoing basis – this means service levels must be included in a contractual agreement. There must be indicators that can trigger exit plan as part of ongoing monitoring.8

iii Existing discrepancies between the GDPR and the PSD2 Directive9 and other financial services regulations

PSD2 and GDPR: a different path to privacy

The PSD210 went live on 13 January 2018, a couple of months before the 25 May enforcement date for the GDPR (which is a regulation and not a directive). The difference may seem minor, but even though the GDPR provides for more than 60 exceptions that can be ruled by national laws, a directive (such as PSD2) is not immediately enforceable under local laws and needs to be transposed. Local laws will hence have a 100 per cent direct impact on the way the PSD2 will be applied throughout the European Union. On top of that, certain terms – and more specifically the regulatory technical standards (RTSs) – of the PSD2 relating to access to data (which is truly the heart of the battle between banks and suppliers) will only come into force in September 2019 – thus creating additional issues from a timing perspective, even without mentioning the fact that these will need to be integrated into local laws.

In addition to the above uncertainties, the GDPR and the PSD2 have a slightly different approach to personal data: while the PSD2 considers that banks and financial institutions should provide access to all of the customers’ personal data in order to stimulate competition and fintech’s innovations, the GDPR’s goal is to empower people and give them back control over their personal data.

This does not mean that there are no legal tools to reconcile both pieces of legislation – such tools include consent and the obligations applicable to the know-your-customer (KYC) rules.

However, once one moves from the high-level principles to implementation, the challenges of reconciling the details of GDPR and PSD2 quickly become obvious.

Consent under the GDPR and the PSD2

A perfect example is obtaining a customer’s consent. The PSD2 allows third-party providers (TPPs) to access the customer’s payment data directly, provided they have obtained explicit consent and use the banks’ infrastructure for the provision of their services. Both pieces of legislation provide for consent but the liability of the party that needs to obtain such consent

8 Article 4.8 of the EBA Guidelines for Cloud Computing: https://eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+ per cent28EBA-Rec-2017-03 per cent29_EN.pdf/e02bef01-3e00-4d81-b549-4981a8f2f1e.
remains unknown. Additionally, while Article 64 of the PSD2 provides that consent may be withdrawn by the payer at any time, but no later than at the moment of irrevocability as defined under Article 80 of the PSD2, Article 7.3 of the GDPR provides that the data subject shall have the right to withdraw his or her consent at any time, including, presumably, the second after it has been given or even before.

While banks are the data controllers and are responsible for implementing safeguards ‘to ensure that they genuinely act on the data subject’s behalf’,11 TPPs are only permitted by the PSD2 to access data as ‘explicitly requested by the customer’ for the sole provision of the services. That means that while TPPs will probably initiate the process of securing customers’ consent, banks will ultimately remain responsible for confirming with, or otherwise separately obtaining, the consent directly from their customers.12

The PSD2 seems, therefore, to ignore the controller-processor-data subject relationship set up in the GDPR.

**Sensitive payment data**

Another interesting example is the definition of the term ‘sensitive payment data’. The RTS on strong customer authentication and common and secure communication under PSD2 states that banks will have to provide account information service providers with the same information available to the customer when directly accessing their account information, provided such information excludes sensitive payment data. However, the terminology has not been defined and is clearly different from the definition of sensitive personal data set out in Article 4 of the GDPR, very much in contrast to US laws where banking information is considered equal to medical data as being especially personal and sensitive. Without further guidance, banks may need to take a more risk-averse approach and redact all data that could possibly fall into the PSD2 definition of sensitive data category in order to avoid breaching rules around data protection, both under PSD2 and GDPR.

**Delay for notifying a data breach**

Article 96 of the PSD2 provides that, in the case of a major operational or security incident, payment service providers shall, without undue delay, notify the competent authority, and the EBA guidelines specify that such notification should be done within four hours. By comparison, the GDPR’s Article 33 requires notification within 72 hours of becoming aware of the breach.

**KYC**

A very common example of the difficulties of implementing the GDPR in the financial industry environment is the processing of criminal data for the purposes of the KYC. Article 10 of the GDPR states that, in order to process criminal records, the data controller must:

a) rely on an Article 6 legal ground (i.e., the legitimate interest); and

b) be authorised under local Member State law.

---


12 This is aligned with the requirements of the UK Open Banking API Standards, available on: https://www.openbanking.org.uk/providers/standards/. For a full review of the various standards, refer to: http://blog.particeep.com/analyse-tout-ce-que-vous-devez-savoir-sur-la-dsp2-et-linfrastructure-api/.

© 2019 Law Business Research Ltd
The KYC is a regulatory obligation imposed on all banks and reinforced in the framework of the fight against money laundering and the financing of terrorism.

In this area, sanctions or the increased threat of sanctions from the authorities have led the banks to strengthen the collection, analysis, and storage of personal data concerning individual consumer customers and executives or shareholders of corporate clients, increasing the volume of data, staff access and exchange of information between entities and suppliers within banks.

The GDPR has several impacts on the KYC:

a. Does the regulation require that the investigation process of the KYC be transparent to the customer, and if so, to what extent?

b. Is there a right for the customer contest and how does the bank avoid liability?

c. How can a bank ensure access to personal data by the data subjects?

d. Will data subjects be able to recover not just all the data provided by themselves to the bank, but also all that generated in the context of the commercial relationship?

e. What retention period shall be applicable?

Specific policies need to be implemented for the KYC by each bank or financial services institution. The many discrepancies between financial regulations and the GDPR force banks and financial institutions to go beyond the requirements of the GDPR, and these discrepancies are echoed on the relationship of the banks and financial institutions with their CSPs to whom they entrust essential IT systems, such as the KYC.

III THE WORK LEFT TO BE DONE BY THE EU COMMISSION

With the globalisation of digitalisation, and the importance gained by cloud computing, the EU Commission may need to generalise banking and financial institutions’ concerns, or at least harmonise the legal and infosec requirements in order to facilitate CSPs’ compliance with the EBA’s requirements.

At the same time, such generalisation should not be detrimental to small and medium enterprises unable to invest as much as the Big Four (i.e., Google, Amazon, Facebook and Apple). In order to achieve such goal, a possible solution would be to implement standardised TOMs that should remain neutral from a technical standpoint and regulate the scope of audits by giving a framework to audits. Auditing should be outsourced to independent companies paid for that, and should not be imposed on a company’s workforce: as much money and time spent on audits cannot be expected out of a small or medium CSP without being seriously detrimental to a fair competition, and CSPs must be able to provide certificates in lieu of on-site audits. Once the issues related to TOMs and auditing are resolved and there is standardisation and harmonisation, subcontracting will probably be much less of a concern.

That being said, there are certain things the European authorities can do.

---

The SCCs

Much has been said and written about the EU SCCs (also known as EU Model Clauses). In fact, there are over 4 million websites that discuss the SCCs in one form or another. However, notwithstanding the introduction of the GDPR, the SCCs in use date back to 2001, 2004 with revision in 2010 (the Controller to Controller SCCs) and 2010 (the Controller to Processor SCCs) and to date have not been updated – and there is no indication that the EU authorities are considering updating the SCCs. However, the SCCs are currently under review as part of a (second) court case brought by Max Schrems in his campaign against Facebook’s data handling policies and procedures.\textsuperscript{14} What follows, therefore, is a consideration of possible changes and updates to the SCCs to bring them into line with GDPR.

Pursuant to Article 26 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 ‘on the protection of individuals with regard to the processing of personal data and on the free movement of such data’ (the Data Protection Directive), the EU created a mechanism to allow for standard contractual clauses to transfer data to third countries that do not have an adequate level of data protection. Accordingly, by Decisions 2001/497/EC and 2004/915/EC, the EU Commission introduced two standard contractual clauses templates between an EU controller and a non-EU or non-EEA controller, and by Decision 2010/87/EU the EU Commission introduced a standard contractual clauses template between an EU controller and a non-EU or non-EEA processor. As has been widely reported and commentated, on 25 May 2018, the GDPR became enforceable after a two-year transition period, and pursuant to Article 46(2) reinforced the right of the EU Commission to adopt SCCs. Unfortunately, no new SCCs have, to date, been issued by the EU to update the existing templates to reflect the requirements of GDPR or the state of progress of technology. This has caused a frenzy of contractual activity, as controllers and processors have had to negotiate their own interpretations of the GDPR’s requirements between them and to the data subject, and while some of the requirements are quite straightforward, others lend themselves to reasonable interpretations. This, along with the general difficulties in managing third-party vendors has resulted in tremendous compliance burdens that could have been alleviated with the issuance of GDPR-ready SCCs.

In addition, the advent of cloud computing has forced certain organisations to review their position on data processing in the cloud. For example, in December 2017 the European Banking Authority issued its Recommendations on Outsourcing to Cloud Service Providers.\textsuperscript{15} This sets out certain baseline requirements for financial service organisations when outsourcing services to cloud service providers.

The SCCs can therefore be considered under threat, and what seems to be an obvious solution is to update them to reflect not only the concerns raised by Schrems but also to reflect the new regulatory landscape as well as current and future technology.

What follows is an examination of some areas with the SCCs that could and should be updated.

\textsuperscript{14} https://iapp.org/news/a/understanding-schrems-2-0/.

**TOMs**

The technical and organisational measures are a huge bone of contention, varying in depth and scope. Much time is spent negotiating these between controllers and processors, where each party insists on using their standard TOMs and eventually a compromise is found. Perhaps the solution is for the authorities to develop a set of TOMs that cover the main key elements minimum standards expected, covering access, input and change, roles, availability, etc.

**Retention period maximum**

A large derogation is the right to retain data. While the GDPR is clear that you should only keep data for as long as it is necessary for the purpose for which it was collected, there is something to be said for introducing a backstop and offering protections for companies that correctly delete the data but might need it to defend against claims, perhaps three years after the contract expires or terminates. The introduction of such a backstop would require a fine balance between the rights, duties and obligations under GDPR versus those imposed by other legal frameworks around statutory limitation periods. One of the conflicts within the GDPR is the right of the data subject to request deletion. If the deletion is granted, an organisation may have difficulty defending against a suit from that same data subject.

**Audit**

The audit right provided in the SCCs is wide and without definition or limitation (Does it refer to allowing access within data center or to company confidential security controls? Does it require a bank's hosting provider to allow the bank's customer to inspect all of its controls in person?) and does not provide any comfort to a processor of the ongoing security of its infrastructure.

Bear in mind, for instance, the technical issues surrounding the simple fact that the temperature of a data centre may be disrupted by the presence of one additional person, putting at risk the data of thousands of customers. How can a regulation grant unlimited on-site audit rights to these same thousands of customers?

The audit right applies regardless of whether the audit is a general one or one following a data incident. For this, perhaps, three streams need to be developed: one audit mechanism for supervisory authorities, and two for the controller (one annual mechanism and a mechanism to handle for auditing following a data breach).

The right to audit should vary depending on the circumstances that resulted in the audit in the first place in order to be meaningful and effective, as an audit is a limited point-in-time view of compliance and arguably less meaningful than contractual promises that are regularly reaffirmed via a questionnaire or a third-party certification. If the purpose of the audit is to evidence compliance, then things such as the requirement for an audit plan, sufficient reasonable advance notice, and the use of mutually agreed upon third-party auditors should be handled via one mechanism. The introduction of GDPR-compliant third-party certifications could go a long way to resolving this issue. An audit following a data breach, by contrast, will more than likely require an abbreviated process recognising the urgency around post-incident compliance, and as such should be done by a single independent auditor, and not all customers coming on-site.
EU Code of Conduct for CSP

Article 42 of the GDPR provides that:

> Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

Adherence to a code is one of the compliance mechanism provided by the GDPR. An EU Cloud Code of Conduct covering the requirements for CSPs is currently being drafted. The Code is:

> designed to be a voluntary instrument, allowing a CSP to evaluate and demonstrate its adherence to the Code’s requirements, either through self-evaluation and self-declaration of compliance and/or through third-party certification. The Code is developed to cover GDPR requirements for a Code of Conduct under GDPR and is being submitted to the appropriate Data Protection Authority.\(^\text{16}\)

While the intention of the EU Cloud Code of Conduct is supposed to make it easier for cloud customers (particularly small and medium enterprises and public entities) to determine whether certain cloud services are appropriate for their designated purpose, it is quite difficult to imagine that it fits the specific needs of micro, small and medium-sized CSPs.

For instance, several references are made to the ISO 27001 standards, but no references are made to projects such as the attempt by the French Agence Nationale de la Sécurité des Systèmes d’Information to ensure that cybersecurity be accessible to everyone, including the micro, small and medium-sized CSPs.

In order to be efficient, we need to make sure this code is not meant exclusively for the Big Four and other large giant tech companies.\(^\text{17}\)

And if we want that to be true, TOMs based on the ISO 27001 standards should be standardised and realistic to put in place from a financial standpoint for all companies.\(^\text{18}\)

Another major essential point that remains unresolved by the EU Code is the ability to proceed to still-required on-site audits, even if the CSP has adhered to the EU Code. The EU Code could have provided that audits be entrusted to independent third parties, coupled with the ability to have certificates to resolve the issues.

It seems, however, that the draft version of the EU Code of Conduct for CSPs has taken a different approach and has left these core issues regarding a pacified relationship between CSPs and banks and other financial institutions unresolved.

For many banks and financial institutions, as well as for providers and companies subject to more than one of the above-mentioned laws, regulations, guidance and directives – and that would comprise a good bit of the ecosystem – the complexity of the legal frameworks coupled with the complexity of the technologies and the savings and efficiencies


\(^{18}\) The ANSSI provides for instance a guide for small and medium companies at [https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-l-informatique/](https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-l-informatique/). Would the respect of such guide be considered as equivalent to the ISO 27001 standards?
from outsourcing leave many practitioners struggling to make sense of the interplay. When discussing with small and medium players, their main preoccupation is that they feel they will never be able to fill the gap required by the regulations, and many give up before even trying to conform to the new standards. The IAPP Annual Privacy Governance Report 2018 highlights that 19 per cent of respondents feel full compliance is impossible; 46 per cent of respondents are concerned of the conflict with other national laws; and 25 per cent of respondents have changed vendors in response to the GDPR.

Time, regulatory actions and, hopefully, guidance will help resolve some of these uncertainties, but a good understanding of the technical issues and the complexity of the legal obligations would certainly be appreciated by most parties.19

Chapter 2

AUSTRALIA

Peter Reeves1

I OVERVIEW

In 2018, the Australian financial services sector 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 sharing of information on fintech market trends, encourage referrals of fintech companies and share insights from proofs of concepts and innovation competitions. ASIC has committed to supporting financial innovation in the interests of consumers by joining the Global Financial Innovation Network (GFIN), which launched in January 2019 and currently has 29 member organisations. GFIN is dedicated to facilitating regulatory collaboration in a cross-border context.

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. In December 2017, ASIC sought industry feedback on the fintech licensing exemption following Treasury consultation on draft legislation designed to enhance the existing exemption.

Investments in fintechs may be made through certain Australian incorporated limited partnerships. Such investments can receive favourable tax treatment. Depending on the

1 Peter Reeves is a partner at Gilbert + Tobin.
investment vehicle chosen, 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.

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 were announced as part of the Federal Budget on 8 May 2018, such as the introduction of an ‘incremental intensity threshold’ proposed by the Treasury Laws Amendment (Making Sure Multinationals Pay Their Fair Share of Tax in Australia and Other Measures) Bill 2018 (Cth). In February 2019, the Federal government released guidelines to clarify the application of the R&D Tax Incentive.

II REGULATION

i Licensing and marketing

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 investment or wealth management business, payment service, advisory business, 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 particular financial product decisions.

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 to hold an ACL. 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 or be entitled to rely on an exemption.

In addition, 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 (e.g., an exchange). Additionally, 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). These 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 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 on customers prior to providing any designated services and adopting and maintaining an AML/CTF programme.

In 2018, the Australian Prudential Regulation Authority (APRA) released the restricted authorised deposit-taking (ADI) framework, which is designed to assist new businesses wishing to enter the banking industry. Under this regime, entities can seek a restricted ADI licence, allowing them to 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. See Section VI.iv for further detail.

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.

Marketing
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) or through delegated powers.

ii Cross-border issues

Passporting

Carrying on a financial services business in Australia will require a foreign financial service provider (FFSP) to hold an AFSL, unless relief is granted. As at the time of writing, Australia has cooperation (passporting) arrangements with regulators in foreign jurisdictions, which enable FFSPs regulated in those jurisdictions to provide financial services they are authorised to provide in their home jurisdiction to wholesale clients in Australia, without holding an AFSL. Before providing financial services, they must disclose to clients that they are exempt from holding an AFSL and that they are regulated 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.

ASIC has announced that it will be proceeding with a proposal to repeal the passport 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 30 September 2019. This is discussed further in Section VIII.

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. The Passport officially launched on 1 February 2019; however, as at the time of writing, Australia is the only participating economy to have passed laws to enable the Passport to operate.

In addition to the Passport, the Corporate Collective Investment Vehicle scheme (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. Public consultation on the third tranche of legislation closed on 26 October 2018 and two draft Bills implementing the CCIV regime were released for public consultation on 17 January 2019.

Australian presence

Foreign companies wishing to carry on business in Australia, including in fintech, must either establish a local presence (i.e., register with ASIC and create a branch) or incorporate 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. Generally, a company obtaining an AFSL will be carrying on a business in Australia and will trigger the requirement.

**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 digital identity technology called ‘GovPass’ is intended to be used with government services with an opportunity for future integration with the private sector. A core component of the GovPass digital identity platform is the identity exchange. The identity exchange uses a double blind and acts as an intermediary between the government service and the identity provider. It ensures that personal information cannot be shared and ensures that the relying party receives an identity assurance that has been verified, without revealing the source of the assertion. In October 2018, the Australian government launched the first pilot of the GovPass digital identity platform, which enables Australians to opt in through a mobile application to apply for a tax file number.

At this stage in the testing of the platform, the extent to which a GovPass digital identity may be used for transactions beyond government services is unknown. The national identity system will be available to Australian residents who can produce their official identity documents, and is predicted to launch in mid-2019.

There is another digital identity service in use in Australia called ‘Digital iD’, which 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, working 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, conditional on 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 used in absence or together with 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, FUNDING AND PAYMENT SERVICES

i 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 Australian Securities and Investments Commission Act 2001 (Cth) (the ASIC Act).

ii 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.

In October 2018, the government passed the Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Bill 2017 (Cth), officially 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.
iii 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 generally 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 market for trading such loans or financings; however, such activities may trigger licensing obligations for the provider of the market, market maker and market participants.

iv Payment services

Payment services may be regulated as financial services, because this 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.

Any entity that conducts banking business, such as taking deposits (other than as part-payment for identified goods or services) or making advances of money, or provides a purchased payment facility, must be licensed as an ADI. APRA is responsible for the authorisation process and granting of ADI licences (as well as ongoing prudential supervision). Recently, APRA released the Restricted ADI framework, which is discussed in Section VIII.

v 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).

Currently, the Australian Privacy Principles (APP) dictate when APP entities may use or disclose personal information. They may do so where an individual could expect for the data to be shared or when an exception applies.

In Australia there has been significant change 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 scheme was introduced; this scheme mandates that entities regulated under the Privacy Act are required to notify any affected individuals and the Office of the Australian Information Commissioner in the event of a data breach (i.e., unauthorised access to or disclosure of information) that is likely to result in serious harm to those individuals.

Additionally, the Australian government announced that it 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. The Open Banking regime is slated to commence in February 2020.

V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

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 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 licences.

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 has long-arm jurisdiction and that the prohibition on misleading and deceptive conduct will 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, an offer of derivatives or fall into a category of more generally defined financial products. 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 relevant disclosure obligations. Additionally, cryptocurrencies are subject to the general consumer protection provisions, whereby providers must not make false or misleading representations or engage in 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. These amendments are 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 will be 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 will also be required to keep certain records relating to customer identification and transactions for up to seven years. The offence for operating a registrable digital currency exchange service without registering with AUSTRAC will carry 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 (such as bitcoin) as neither money nor a foreign currency. Under Australian income tax laws, gains made on the disposal of cryptocurrencies (including where cryptocurrencies are used as the payment for services or goods) contribute to the taxable income of a taxpayer. The ATO’s views on the income tax implications of transactions involving cryptocurrencies is in a state of flux owing to the rapid evolution of both cryptocurrency technology and its uses.

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.

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.

### 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.

### 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 1959 (Cth). 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 term ‘neobank’ is largely a fluid construct, but generally, these entities will use an internet or mobile platform to interact with customers and offer a different user experience from a traditional bank. For example, the ability to make mobile deposits, person-to-person payments using email addresses or phone numbers, real-time digital notifications of receipts, no monthly fees, no automated teller machines fees and intuitive budgeting tools are typical characteristics of a neobank.

The Australian banking sector is highly regulated, with stringent licensing and reporting requirements. Consequently, neobanks face significant regulatory challenges entering the market. Under Australia’s current regulatory framework, APRA prohibits ADIs, with less than A$50 million in capital, from using the word ‘bank’. In 2018, APRA released the Restricted ADI framework, which is designed to assist new businesses to enter the banking industry. Under this regime, entities can seek a Restricted ADI licence, allowing them to 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 or exit the industry.

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.
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

The Privacy Act regulates the handling of personal information by Federal government agencies and private sector organisations with an aggregate group revenue of at least A$3 million. The Privacy Act includes 13 APPs, which create obligations on the collection, use, disclosure, retention and destruction of personal information.

In 2018, the Australian Government announced that 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. These sharing arrangements are intended to facilitate easier swapping of service providers, enhancement of customer experience based on personal and aggregated data, and more personalised offerings.

Additionally, the European Union (EU) General Data Protection Regulation has extremely broad extraterritorial reach and may significantly impact the data handling practices of Australian businesses offering goods and services in the EU.
VIII YEAR IN REVIEW

i Royal Commission

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. The Royal Commission’s findings of misconduct have resulted in a marked decrease in consumer trust in both the traditional financial services industry generally and the institutional ability to prioritise customer needs, with 42 per cent of customers acknowledging that trust in banks had deteriorated significantly over the past year.

Traditional financial services providers were not the only targets of the Royal Commission with corporate regulators generating criticism 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. In keeping with its broader strategic change to strengthen its governance and culture, ASIC plans to implement all recommendations from the Royal Commission that were directed at ASIC and require no legislative change. Significantly for businesses, the Treasury Laws Amendment (Strengthening Corporate and Financial Sector Penalties) Act 2018 (Cth) has commenced and provides ASIC with additional penalty provisions to provide greater deterrence value. ASIC has also stated that it will establish a separate Office of Enforcement within ASIC in 2019 to centralise decision-making processes when determining whether to commence enforcement action.

ii Asia Region Funds Passport regime

See Section II.ii for details of the Asia Region Funds 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) has recently received Royal Assent. 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 Tiered marketing licensing regime

In May 2018, ASIC introduced a two-tiered licensing regime for financial markets and updated corresponding regulatory guidance. Specifically, the guidance reflects the risk-based assessment that will take an internationally consistent approach to the administration of the market licensing regime. Under the market licence regime, market venues can be designated as either Tier 1 or Tier 2 licensees, depending on their nature, size, complexity and the risk they pose to the financial system, investor confidence and trust.

Generally, Tier 1 market venues are, or are expected to become, significant to the Australian economy or the efficiency and integrity of (and confidence in) the financial system. Tier 2 licences will be able to facilitate a variety of market venues, including specialised and emerging market venues, and will have reduced licence obligations to accommodate new and specialised market platforms.

The tiered market licence regime is expected to impact, among others, market operators and operators of market-like venues (i.e., those that facilitate financial product trading on the basis of being exempt from the Corporations Act requirement), as well as platforms seeking to offer secondary trading.

v Passport relief

In late 2018, ASIC announced that from 30 September 2019 it will no longer allow FFSPs to rely on ‘passport’ class order relief or on ‘limited connection’ relief from the requirement to hold an AFSL in order to provide financial services in Australia to wholesale clients. Instead, ASIC will be proceeding with its proposal to implement a new regime that will require FFSPs to apply for a foreign AFSL. FFSPs currently relying on passport relief will have 12 months to transition to a foreign AFSL or satisfy licensing requirements in some other way. ASIC plans to release, in the first half of 2019, a draft Regulatory Guide and draft instruments relating to the foreign AFSL regime.

vi Restricted ADI

An entity that conducts any banking business, such as taking deposits (other than as part-payment for identified goods or services) or making advances of money, must be licensed as an ADI. In 2018, APRA released the Restricted ADI framework, which allows new businesses entering the banking industry to conduct a limited range of banking activities for two years while they build their capabilities and resources. See Section VI.iv. for further detail.

IX OUTLOOK AND CONCLUSIONS

There has been a variety of regulatory and legislative developments in the fintech industry, with 2019 bringing further developments that are likely to have an ongoing impact on 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 incoming Asia Region Funds Passport regime and the commencement of open banking, fintech is likely to have greater opportunities for growth as the sector moves from speculation to development to implementation.

While the government continues to promote fintech investment and innovation, consumer protection remains a central focus point for 2019. Following the findings of the Royal Commission’s Final Report, there is likely to be a greater focus on service over sales
across the financial services sector and corporate regulators will look to financial service providers to comply with the law in a way that is consistent with broader and developing community expectations. We expect to see more rigorous engagement with ASIC and APRA during licence application processes, and for non-compliance to be dealt with in a way that is prompt and firm.

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 consumer demand for bespoke offerings and tailored customer services, while established institutions face the challenge of redesigning their existing commercial strategies and capabilities.
Chapter 3

AUSTRIA

Oliver Völkel and Bryan Hollmann

I OVERVIEW

Fintech continues to be a vibrant and fast-developing industry in Austria. The industry enjoys the support of the government, which has actively sought to provide legislative and regulatory clarity to attract fintech businesses to the country. Since 2016, the government’s priorities in the fintech industry have been shaped by the Blockchain Roadmap of the Federal Ministry of Education, Science and Research, as well as the Digital Roadmap of the Federal Ministry for Digital and Economic Affairs. More recently, the newly established fintech advisory board, an initiative of the Federal Ministry of Finance, approved the establishment of a regulatory sandbox, which is anticipated to go live in the first half of 2019. Participation will be limited to companies licensed by the Austrian Financial Market Authority (FMA) or the European Central Bank as well as companies potentially to be licensed by the FMA. Further regulatory proposals are expected by the fintech advisory board in the course of 2019.

Licensing requirements for companies in the financial services industry in Austria are strict and multifaceted. To provide support to fintech companies in particular, the FMA maintains the FinTech Navigator, a publicly available online resource that provides general overviews of licensing obligations and other topical regulations. The FMA also makes itself available via the FinTech Point of Contact to answer informal questions on legal issues pertinent to fintech companies such as licensing, prospectus requirements and compliance and anti-money laundering regulations. More formal applications to the FMA for notice of a binding legal opinion are also possible.

Small to medium-sized fintech companies may utilise the same tax incentives and funding sources generally available to start-ups. Austria hosts a dynamic start-up scene that is home to numerous incubators and accelerators, particularly in the capital, Vienna.

1 Oliver Völkel is a founding partner and Bryan Hollmann is counsel at Stadler Völkel Rechtsanwälte GmbH. The authors would like to thank Arthur Stadler, Andreas Pfeil, Jacqueline Bichler and Margaux Mermin for their valuable contributions.


II REGULATION

i Licensing and marketing

There is no special licensing regime for fintech companies in Austria. Austrian supervisory laws are technology-neutral, which means that each company’s business model and the scope of its business activities must be examined on a case-by-case basis to determine whether a licence is required. Licensing is primarily conducted by the FMA.

Fintech companies active in Austria should consider whether the following licences are applicable to them:

a licence pursuant to Article 1(1) of the Banking Act (BWG) for engaging in banking transactions;

b licence pursuant to Article 3(2) of the Securities Supervision Act 2018 (WAG) for providing investment services;

c licence pursuant to Article 1(2) of the Payment Services Act 2018 (ZaDiG) for providing payment services;

d licence pursuant to Article 1(1) of the E-Money Act 2010 for issuing electronic money;

e licence pursuant to Article 4(1) of the Alternative Investment Fund Managers Act (AIFMG) for managing an alternative investment fund;

f licence pursuant to Article 6(1) of the Insurance Supervision Act 2016 for pursuing contractual insurance activities; and

g obligation pursuant to Article 2(1) of the Capital Market Act (KMG) to publish a prospectus.

The obligation to obtain a licence applies to companies that operate on a commercial basis and are active in Austria. Companies incorporated outside of Austria are deemed to be active in Austria if their business model actively targets the Austrian market, which can be evidenced by, inter alia, maintenance of an Austrian website (.at domain), providing Austrian contact information, advertising in Austria or establishing an Austrian distribution network. The seat of the company and the origin of its services are not determinative, but rather the active targeting of the Austrian market or the destination of the company’s services to customers or investors in Austria.

Many common business models and activities in the fintech industry are susceptible to triggering a licence obligation in Austria. For example, issuers of initial coin offerings (ICOs) must be particularly mindful of licence requirements, as blockchain technology makes it easier than ever to engage in regulated activities over the internet with few, if any, gatekeepers or other intermediaries. Also, cryptocurrency mining companies that passively manage capital gathered from a number of investors may be regarded by the FMA as alternative investment fund managers under the Austrian AIFMG if offered within or into Austria. Internet-based platforms that provide investment or brokerage services may require a licence pursuant to the WAG. There are no special rules for companies that offer automated investment advice and trading. The FMA does not hesitate to initiate administrative proceedings against companies engaged in unauthorised business practices.

Other fintech business models that are gaining popularity in Austria, such as platforms for trading contracts for difference (CFDs) and binary options, are currently in a state of regulatory flux. On the EU level, the European Securities and Markets Authority (ESMA) temporarily banned the marketing, distribution or sale of binary options to retail clients. The ban has been in force since 2 July 2018 and will remain in force until at least 2 July 2019.

© 2019 Law Business Research Ltd
ESMA has similarly placed restrictions on CFDs, which will remain in force until at least 1 May 2019. In Austria, it is currently unclear whether offering binary options or CFDs settled in cryptocurrencies are subject to an investment services licence under WAG.

The standards for obtaining a financial services licence in Austria are consistent with the standards set by applicable European legislation. Once an application for a licence has been made, the FMA typically has three months to make a decision or request additional time for review. Formal and informal means of communicating with the FMA regarding the applicability of one or more licences in a particular case are available.

Even if a licence pursuant to Austrian supervisory law is not required, a general licence obligation under the Trade Act (GewO) may nevertheless exist. Trade licences are administered by local authorities and are required to carry out any kind of trade or business activity in Austria. There are two types of trades: free and regulated. Licences for regulated trades as listed in the GewO are subject to more stringent requirements, including providing a certificate of professional competence. Businesses providing temporary cross-border services pursuant to the EU’s freedom to provide services are subject to special rules under Section 373a GewO but are exempt from the requirement to provide a certificate of competency.

Marketing of fintech products and services are subject to the same rules as other financial industry participants. In particular, clients of investment firms are entitled to adequate information that is fair, clear and non-misleading in order to make informed investment decisions. These principles also apply to marketing communications (Article 40(7) WAG). Moreover, issuers of securities or investments must take care that marketing materials do not run afoul of the prohibition against offering securities or investments, for which no approved prospectus has been published pursuant to the KMG.

ii Cross-border issues

Companies within the European Economic Area (EEA) may passport certain EU-regulated or licensed activities from another jurisdiction into Austria pursuant to the single licence principle. The process is relatively simple: companies must first notify their home supervisory authority, which then notifies the FMA. The same applies vice versa if a licensed Austrian company intends to provide services in another jurisdiction within the EEA. The FMA maintains a searchable list of companies authorised to be active on a cross-border basis on its website. The single passport is available for regulated companies under, inter alia, the Capital Requirements Directive, the Markets in Financial Instruments Directive (MiFID II), the Payment Services Directive and the Alternative Investment Fund Managers Directive (AIFMD).

If a company intends to offer services cross-border pursuant to the EU’s freedom of establishment, the establishment of a local branch is required. No local branch is required if cross-border business is conducted pursuant to the EU’s freedom to provide services.

Reverse solicitation, the provision of regulated services by a third-country firm upon the exclusive initiative of a retail or professional client, is possible in theory pursuant to MiFID II or the AIFMD; however, the FMA interprets the applicable exemptions narrowly.

The Oesterreichische Nationalbank (OeNB), the central bank of Austria, administers foreign capital exchanges under the Foreign Exchange Act 2004. Except for certain cases referred to in the Treaty on the Functioning of the European Union, capital transactions and

payments with other countries are not subject to any restrictions. However, the OeNB retains the authority to take certain measures to fulfil its obligations under international law or to safeguard the foreign interest of Austria. Under the Foreign Trade Act 2011 (the AußWG 2011), the acquisition of a 25 per cent or more shareholding of a company active in an area of public safety and order by certain foreign persons requires prior approval by the federal ministry in charge of economic affairs.

III DIGITAL IDENTITY AND ONBOARDING

Austria generally recognises two forms of digital identification: the Mobile Phone Signature and the Citizen Card. Both can be used to electronically sign documents in PDF format such as contracts or receipts. These electronic signatures have the same legal validity as handwritten signatures. Austrian citizens and residents generally are eligible for both services.

Financial service providers have been able to carry out fully digitised onboarding of clients since 3 January 2017. The FMA’s Online Identification Regulation sets out strict organisational and procedural safeguards for video-based online identification, which effectively require digitised onboarding to be conducted in a live (rather than pre-recorded) setting. To complete the verification process, a potential customer must, inter alia, provide a screenshot of his or her face as well as the front and back of an official photo identification document. The potential customer must also upon request move his or her head while showing his or her face and communicate the serial number of the official photo identification document. Specially trained staff are required to conduct the online identification process in a separate room equipped with an access control system. Owing to these stringent requirements, many financial service providers outsource digitised onboarding to third parties.

IV DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES

i Collective investment schemes

Management of a collective investment scheme generally requires a licence in Austria. Several regulatory classifications are possible, depending on the structure of the scheme. A licence determination frequently turns on whether an investment strategy is present and whether the collected funds are directly attributable to operational activity.

Managing an alternative investment fund requires a licence pursuant to the AIFMG unless total assets under management do not exceed certain thresholds, in which case mere registration with the FMA is required. Without a licence, however, an alternative investment fund manager is prohibited from marketing any alternative investment fund to retail investors and engaging in cross-border marketing or management.

Undertakings for collective investment in transferable securities (UCITS) in Austria are governed by the Investment Fund Act 2011 (InvFG 2011), which transposes the UCITS Directive. The InvFG 2011 also regulates special types of alternative investment funds such as pension investment funds.

The management of real estate investment funds is also subject to a licence pursuant to the Real Estate Investment Fund Act. As such funds are a subtype of an alternative investment fund, the provisions of the AIFMG are also applicable.
ii Crowdfunding

Crowdfunding projects that publicly offer securities or investments in Austria are subject to the requirement to publish a prospectus pursuant to the KMG. The FMA reviews prospectuses for offerings of securities such as traditional stocks or bonds, while offerings of investments – essentially transferable, securitised rights that are not securities – are reviewed by a non-governmental prospectus auditor of the issuer’s choice. Donation and rewards-based crowdfunding are generally not subject to the prospectus requirement. Certain offerings are exempt from the obligation to publish a prospectus.

Small and medium-sized enterprises may take advantage of special crowdfunding rules under the Alternative Financing Act (AltFG), which is enforced by the local administrative authorities rather than the FMA. Generally, under the AltFG, public offerings with a total consideration of up to €250,000 within 12 months have no prospectus or information requirement. Public offerings that lead to a total consideration from more than €250,000 to less than €2 million within 12 months must provide investors with an information sheet set out in the Alternative Financing Information Regulation. Public offerings exceeding €2 million and up to €5 million require a simplified prospectus in accordance with Annex F of the KMG. Retail investors in offerings pursuant to the AltFG generally cannot invest more than €5,000 within a 12-month period.

Crowdfunding platforms should be mindful of potential licence obligations if they engage in certain business activities such as providing brokerage or investment services (WAG), payment services (ZaDiG) or engage in banking transactions such as credit intermediation (BWG). The AltFG contains specific requirements for operators of an internet platform related to the prevention of money laundering and terrorist financing and transparency of information. Platforms therefore often engage licensed partners to provide such regulated services.

iii Lending

The conclusion of money-lending agreements and the extension of monetary loans requires a licence pursuant to Article 1(1) No. 3 BWG. No special exemptions exist for peer-to-peer lending.

V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

i Cryptocurrencies

To date, Austria does not have a specific regulation for blockchain technology. The FMA generally views cryptocurrencies, namely, bitcoin and its ilk, as falling outside its regulatory purview since cryptocurrencies are not legal tender and not backed by a central authority. Nevertheless, the FMA has actively warned consumers of the high financial and technological risks posed by cryptocurrencies.

The Austrian government has been considering how to approach the regulation of cryptocurrencies over the past year. In February 2018, Finance Minister Hartwig Löger announced his position that cryptocurrencies should be regulated similar to gold and derivatives, which are subject to robust anti-money laundering and counter-financing of terrorism (AML and CFT) rules. To this end, Austria supports the amendment to the EU

---

6 https://www.bmf.gv.at/presse/LoegerKryptowaehrungen.html.
Anti-Money Laundering Directive (the 5th AMLD), which must be implemented into national law by 10 January 2020. The 5th AMLD extends the scope of application of AML and CFT rules to include custodian wallet providers and platforms for exchanging virtual currencies. The newly established fintech advisory board in Austria may produce more specific recommendations on how cryptocurrencies should be regulated. In any case, it appears that the current Austrian approach is to wait for further guidance on the European level.

This does not mean that cryptocurrency-related businesses are free from regulation. Companies that transact in cryptocurrencies may require a licence if they engage in certain activities (see Section II.i). Issuers of payment tokens, for example, may require a licence for the issuance and administration of payment instruments pursuant to Article 1(1) No. 6 BWG. With regard to cryptocurrency mining, mining cryptocurrencies in one’s own name and on one’s own account generally does not require a licence, although certain business models may qualify as an alternative investment fund under the AIFMG.

Austria’s approach to cryptocurrency taxation is generally favourable to investors and consumers. Cryptocurrencies held by natural persons as business assets are subject to income tax at applicable rates prescribed in the Income Tax Act. Conversely, gains on cryptocurrencies held as non-business assets for longer than one year are tax free. In line with the seminal Hedqvist ruling by the Court of Justice of the European Union, the exchange of fiat currency into bitcoin and comparable cryptocurrencies and vice versa is exempt from VAT. Cryptocurrencies obtained by mining are treated in the same way as the production of other assets for taxation purpose. Operating a cryptocurrency ATM also has tax consequences.

ii Initial coin offerings

The FMA is open-minded toward capital-raising projects using blockchain technology. In November 2018, the FMA approved for the first time a prospectus for an offering of securities executed on the basis of blockchain technology in the EU.7 The prospectus was successfully passported into Germany.

The FMA roughly classifies tokens offered in ICOs into three categories: security and investment tokens, payment and currency tokens and utility tokens.

Security and investment tokens are subject to the requirement to publish a prospectus. Depending on the rights attached to the token, security tokens may represent transferable securities or investments. The term ‘transferable securities’ is defined in MiFID II and is transposed into Austrian law through the KMG and WAG. Generally, tokens qualify as transferable securities if they resemble traditional securities such as bonds, shares or profit participation rights – a popular type of security in Austria that resemble shares but exclude voting rights. If transfer of a token is restricted but certain rights are embodied on the token and risk-sharing within a group is present, the token may qualify as an investment.

Payment and currency tokens are not subject to the requirement to publish a prospectus, but issuers of payment tokens may require a licence for the issuance and administration of payment instruments. A licence is not required if the payment system constitutes a limited network.

Utility tokens with features that overlap with security or payment tokens are subject to the respective regulations outlined above. In Austria, utility tokens typically resemble

---

7 The authors represented the issuer in the prospectus.
vouchers that entitle holders to goods or services available on a (yet-to-be developed) platform. The FMA views this model as comparable to a payment token; however, most models are exempted from the licence requirement on the ground of the limited network exemption.

VI OTHER NEW BUSINESS MODELS

i Self-executing contracts
Self-executing contracts, colloquially known as ‘smart contracts’, entail significant legal uncertainty. As there is no special legal framework for smart contracts, foundational principles of contract formation under Austrian private law apply. It is currently not possible to conclude certain types of agreements entirely via smart contracts, as Austrian law requires certain formalities such as notarisation to be kept. Enforcement issues that are likely to arise, particularly with regard to the reversal of immutable transactions and the conclusion of agreements with anonymous or pseudonymous parties, have yet to be resolved by the courts.

ii Decentralised exchanges
Decentralised exchanges that permit peer-to-peer trading of security tokens without a central intermediary are not exempt from the licence requirement for the operation of a multilateral trading facility under Article 1(2)(h) WAG.

iii Proof of stake algorithms
The transition of some popular cryptocurrencies from a proof of work to a proof of stake consensus algorithm may raise novel legal issues in Austria. In a proof of stake system, nodes validate transactions based on the amount of coins held. To maximise its ability to validate transactions, a node may borrow coins from other network participants in exchange for interest. Whether this practice triggers a licence obligation for deposit, lending or custody businesses under the BWG is unclear. The FMA has not explicitly addressed the issue.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

i Intellectual property
Austria does not have special rules that protect an entire business model per se. Accordingly, business models must be examined on a case-by-case basis to determine whether any intellectual property rights can be protected. The most relevant available protective rights under Austrian law include:

a trademarks protected under the Trademark Protection Act;
b designs protected under the Design Protection Act;
c patents protected under the Patent Act;
d utility patents protected under the Utility Patents Protection Act; and
e copyrights protected under the Copyright Act (UrhG).

Protection afforded under the above legislation is usually provided by registration in a public register and lasts up to 70 years after the death of the author.
Software protection

Software is protected as a work of literature under Section 40a UrhG if it is the result of the own intellectual and individual creation of its author or their authors and has a minimum level of creativity and complexity. This protection includes the machine-, object- and source-code of the software, as well as design material such as flowcharts or structure charts. However, graphic user interfaces of a software as well as the ideas and principles underlying the software are not protectable. The author of the software is always its creator. Legal entities are excluded as creators. It is possible to transfer derived rights of use to legal entities. For this reason, rights owners within the meaning of the UrhG are always only natural persons. In view of the complexity of today's software and its programming, co-ownership can be assumed. The UrhG may also protect databases under certain circumstances.

Unless otherwise agreed, only the employer is entitled to exercise property rights in software that was developed by an employee within the framework of an employment agreement. The employer thus effectively receives a legally required licence.

The unauthorised duplication and distribution of software can be prosecuted civilly for damages and injunctive relief as well as criminally by private prosecution.

Data protection

The EU General Data Protection Regulation (GDPR) has been legally binding and directly applicable throughout the EU since 25 May 2018. In Austria, the Data Protection Act (DSG) further implements certain provisions of the GDPR.

The GDPR generally applies to the processing of personal data related to identifiable natural persons. The processing of client data of fintech companies is therefore also covered within the scope of the GDPR.

Persons who deal with the processing of personal data must implement appropriate technical and organisational measures and procedures to ensure that the rights of persons concerned are adequately protected. Pursuant to Article 33 GDPR, personal data breaches of a certain nature must be reported to the Austrian Data Protection Authority (DPA) within 72 hours after having become aware of it. Moreover, the person whose rights were violated must be informed without undue delay if there is a high risk to their personal rights and freedoms.

Digital profiling of clients is covered under the GDPR. Fintech companies must take into account that, at the time the data used for profiling is collected, data subjects are entitled to certain information including the fact that the profiling is taking place, the legal justification for the profiling and the expected effects of the profiling. Furthermore, a data protection impact assessment must be carried out if a systematic and extensive evaluation of personal aspects relating to natural persons is conducted (Article 35(3) GDPR). The persons concerned have the right to object pursuant to Article 21 GDPR, according to which the person concerned may, among other things, object to profiling if profiling is based on the legal basis of the overriding legitimate interest or is carried out for the purposes of direct marketing.

Fintech companies may be required under certain circumstances to conduct a data protection impact assessment, to compile a list of processing activities and to appoint a data protection officer. The DPA may impose fines of up to €20 million or, in the case of a company, up to 4 per cent of its total annual worldwide turnover in the previous financial year.

The provision of banking secrecy pursuant to Article 38 BWG is also of significance to fintech companies. According to this provision, credit institutions, their shareholders, board
members, employees and other persons working for credit institutions may not disclose or utilise secrets or sensitive information that have been entrusted to them or made accessible to them exclusively on the basis of business relations with customers. In contrast to the GDPR, the BWG protects legal entities. Even if a transfer of data is not subject to banking secrecy or is permissible under the BWG, its admissibility under the GDPR or the DSG must also be examined. In the event of a breach of banking secrecy, fintech companies may also be liable under civil, criminal and administrative laws.

Further data protection regulations are contained in the Austrian Telecommunications Act.

**VIII YEAR IN REVIEW**

The establishment of the fintech advisory board by the Federal Ministry of Finance in April 2018 was a welcome development that may accelerate the pace of fintech regulation in Austria. The advisory board has already approved regulatory sandboxes for certain regulated entities, which are expected to go live in the first half of 2019. Further regulatory proposals are expected by the fintech advisory board in the course of the year.

The FMA has been supportive of capital raising projects using blockchain technology. In November 2018, the FMA approved for the first time a prospectus for an offering of securities executed on the basis of blockchain technology. More projects of a similar nature are expected to follow.

**IX OUTLOOK AND CONCLUSIONS**

In addition to the regulatory sandboxes, the Federal Ministry of Finance has identified two other priorities for the fintech industry in 2019:

- the creation of a central platform for financial companies to manage know-your-customer data of customers; and
- the dematerialisation of securities.

These priorities align with the Finance Ministry’s larger goal of digitalising the financial services sector. The time to implementation, however, is uncertain. In any case, the Austrian government will be tasked in the course of 2019 with transposing the provisions of the 5th AMLD into national law by the 10 January 2020 deadline. The future of cryptocurrency regulation in Austria, namely whether cryptocurrencies will be regulated like gold and derivatives, remains to be seen. In any case, Austria is likely to follow guidance provided on the EU level.
Chapter 4

BELGIUM

Pierre E Berger, Stéphanie Liebaert and Marc Van de Looverbosch

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. 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:

a Directive 2015/2366 of 25 November 2015 ‘on payment services in the internal market’ (PSD II);
b 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);
c Directive 2014/65/EU of 15 May 2014 ‘on markets in financial instruments’ (MiFID II); and
d 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. However, the financial regulators have identified fintech as an important focus of their supervisory activities and...
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).4 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.5

The financial regulators are also supporting partners of B-Hive, a Belgian collaborative innovation fintech platform. The platform was launched as a consequence of the Report of the High Level Expert Group established at the initiative of the Minister of Finance of Belgium. This fintech platform brings together major banks, insurers and market infrastructure players, works on common innovation challenges and builds bridges to the start-up and scale-up community.6 Another important platform fostering and promoting the Belgian fintech sector is FinTech Belgium, a community for financial professionals, start-up entrepreneurs and investors.7 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. According to B-Hive, the fifth-highest number of fintech deals in Europe in 2017 took place in Belgium.

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 29.58 per cent (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 4.43 per cent (3.75 per cent as from 2020). 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.

---

6 See https://b-hive.eu/about-us.
7 See https://fintechbelgium.be/.
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;
- yearly turnover (excluding VAT): < €700,000; and
- 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 40 per cent or 80 per cent of the withholding tax on remunerations paid to researchers holding specific 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 29.58 per cent of the invested amount (25 per cent as from 2020). 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 into young companies may recover 25 per cent of the invested amounts by means of a tax credit. This measure is aimed at supporting companies’ efforts in raising 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. Scale-ups cannot attract more than €500,000 through this regime (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.

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).8 The new Anti-Money Laundering Directive9 (AMLD V), which has not yet been implemented in Belgium, specifically provides that electronic identification means can be used to identify the customer and verify his or her

---

8 Regulation 910/2014 of 23 July 2014 ‘on electronic identification and trust services for electronic transactions in the internal market’.

identity if the eIDAS Regulation is complied with or if another secure, remote or electronic identification process is used that is regulated, recognised, approved or accepted by the relevant national authorities.\(^{10}\)

### IV DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES

#### i Crowdfunding

Various types of crowdfunding platforms exist on the Belgian market:

- platforms through which the public makes a donation for a project or enterprise;
- platforms through which the public deposits money in order to receive a non-financial compensation (reward-based crowdfunding);
- platforms through which the public invests in a project or enterprise through a loan (loan-based crowdfunding, also referred to as crowd-lending); and
- 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:

> the 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

\(^{10}\) 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:

- services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account;
- services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account;
- 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);
- 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);
- issuing of payment instruments and acquiring of payment transactions;
- money remittance;
- payment initiation services; and
- 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:

- the limited network exemption;
- the commercial agent exemption; and
- 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 AND INITIAL COIN OFFERINGS

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. These documents, as discussed in this section, are the only forms of regulatory guidance in Belgium that specifically address tokens and cryptocurrencies.

---

11 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 list
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. 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.

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). In this text, which is considered soft law, the FSMA endorses the statements by the European 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. The FSMA further states that the following legislation and regulations may apply to ICOs in Belgium:

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;

b the Marketing Prohibition Regulation (discussed above); and

c the Crowdfunding Act (discussed above).

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:

[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

of cryptocurrency trading platforms in respect of which it has received questions or complaints from consumers and has identified signs of fraud (see https://www.fsma.be/en/warnings/companies-operating-unlawfully-in-belgium).

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’.

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.


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.

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{16} 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*{ii General laws and regulations that may apply to tokens and cryptocurrencies}

\textbf{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.

\textbf{Prospectus regime}

The Belgian prospectus legislation, among others:

\begin{enumerate}
\item 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;
\item establishes a monopoly on intermediation for the placement of investment instruments within the territory of Belgium; and
\item determines that advertisements used in connection with the public offering must receive prior approval from the FSMA.
\end{enumerate}

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.  

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).

**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). 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 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

---


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


20 Robby Houben, ‘Bitcoin: there are two sides to every coin’ (2015) 2 TBR 139, 153 Paragraph 32.
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.21

**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, provided the validity requirements under Belgian contract law are met.22 Some tentative attempts to analyse smart contracts under Belgian contract law have thus far been made, but a considerable degree of legal uncertainty remains.23

**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.24 According to Roland Berger, the Belgian market is expected to grow significantly to €3.7 billion assets under management by 2022.25 Financial regulation, such as MiFID II, apply to automated investment advice as they

---

21 See https://www.ruling.be/fr/telechargements/liste-de-questions-crypto-monnaies.
25 id.
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.\(^{26}\)

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.\(^{27}\) 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 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.\(^{28}\)

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

\(^{26}\) 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.

\(^{27}\) See https://www.fsma.be/en/fintech-contact-point.

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 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 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 in order to safeguard the rights of individuals.

On 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 a significant growth in 2017.\footnote{FSMA, ‘Equity and debt-based crowdfunding in Belgium: Developments over the 2012–2017 period’, https://www.fsma.be/nl/news/crowdfunding-groeit-gestaag-belgie (accessed on 13 March 2019).} 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 be implemented in Belgium by 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 5

BRAZIL

Alexei Bonamin, Carla do Couto Hellu Battilana, Ivan Antonio Monteiro Marques, Maria Eugenia Geve de Moraes Lacerda, Thaís Helena Valente Teixeira Lima and Victor Cabral Fonseca

I OVERVIEW

Brazilian financial technology (fintech) has developed considerably in recent years. The latest version of FintechLab Radar (August 2018) demonstrated a growth of 21.4 per cent in the number of total companies acting in this market, compared with the previous edition published in November 2017. According to the mapping created by the publication, Brazilian fintech operates in 10 different sectors: payments, financial management, credit and loans, investment, insurance, funding, data collection, cryptocurrency and distributed ledger technology (DLT), exchange and multiservices. Among these, the loans and insurance sectors performed the highest growth rates – 92 per cent and 75 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 equivalent of the 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. 588/17, 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.

Although there is no regulation regarding the whole fintech sector, nor any tax incentives, there has been a significant increase in the activities, organisation and protagonism of such companies. 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.

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 are 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.

---

1 Alexei Bonamin and Carla do Couto Hellu Battilana are partners and Ivan Antonio Monteiro Marques, Maria Eugenia Geve de Moraes Lacerda, Thaís Helena Valente Teixeira Lima and Victor Cabral Fonseca are associates at TozziniFreire Advogados.
II REGULATION

i Licensing and marketing

Brazilian legislation does not provide a specific type of operating licence for fintech. 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 elaborated 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, to regulate the segment of 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, futures;
c SUSEP for the insurance industry; and
d the National Complementary Pension Superintendence (PREVIC), for the private closed pension funds segment.

Thus, 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, 476, 555 and 578, and others), asset management (the most

---

2 For a detailed description of the composition of the National Financial System and functions of each entity, see www.bcb.gov.br/Pom/Spb/Ing/InstitucionalAspects/TheRoleFinancialIntermediaries.asp (in English).

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 from this market.

4 Like Central Bank Resolution No. 4.122/2012, that establishes the procedures for the licensing and authorisation granting multiple kinds of banks.
important being CVM Rule No. 558) and investment advisory services (represented by the recently edited CVM Rule No. 592). The use of automated systems or algorithms is permitted for both asset management and advisory activities.

Another industry commonly associated with fintech recently admitted by the Brazilian legal system is investment-based crowdfunding, which is now regulated according to CVM Rule No. 588/17. 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 Defense 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 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 operations 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. 588/17), which is inspired by the regulatory approach used in the European Union, France, the United Kingdom, the United States, Portugal and Canada, among others.

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

---

5 Article 16-A, CVM Rule No. 558/15.
6 Article 16, CVM Rule No. 592/17.
7 See Law No. 4.595/64.
the country, which determines that foreign banks may operate in Brazil if registered within the Central Bank and explicitly authorised by a decree from the executive branch (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 legal entity headquartered in Brazil and authorised by the CVM.8 The same applies to investment advisers,9 who also need entity authorisation to carry out their activities.

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. 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.

III DIGITAL IDENTITY AND ONBOARDING

In the second half of 2018 and in early 2019, there were few regulatory changes regarding the identification of Brazilian citizens. However, some relevant developments are in sight.

There are some 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.

Considering the use of documents by financial service providers, the scenario remains almost the same. BACEN Resolution No. 4.474/16 authorises institutions to discard the use of physical versions once they are digitised and secured within their systems. Financial institutions are also authorised to perform onboarding of clients using a fully digitised process, as provided by BACEN Resolution No. 4.480/16. According to this Resolution, companies must adopt high-security procedures in the opening of accounts by electronic means, in order to guarantee the authenticity of the information and the identity of the proponents.

The only change with regard to digital onboarding comes from a presidential decree issued in February 2019 that makes the taxpayer registry identification number enough for identification purposes for access to information and services and 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.

---

8 Among other prerequisites. See CVM Rule No. 558/15.
9 See CVM Rule No. 592/17.
IV DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES

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 involving national companies or individuals. All regulations regarding the SFN applies to fintech organisations, if legally prescribed services or products are offered.

Recently, Brazilian authorities have legally recognised investment-based crowdfunding as a possible fundraising option for companies that the Rule considers small. Now, the Brazilian innovation ecosystem uses a Rule created specifically to regulate the distribution of securities through platforms established for this purpose, without the need to register this offer with the CVM – which is usually the rule and may be very expensive for small companies. The standard came into force in 2017 following a public consultation of the market conducted by the entity, and its current version determines some requirements and responsibilities for the operation of the platforms, details of the possible offers and recognises the possibility of syndicated investments, that is, the ones led by an investor with a high reputation in the market.

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 then is subject to the supervision and regulation of the BACEN. In order to foster innovative lending models, the entity in 2017 proposed a public hearing that deals with peer-to-peer 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. 4.656/18, which created two special types of financial institutions that are allowed to use electronic platforms to match creditors and borrowers (SEPs) or to lend their own resources (SCDs). Both need to request before the Central Bank authorisation to operate, but they represent a softer, easier and faster process than the one required to traditional financial institutions.

Payment services are subject to the rules regarding the Brazilian payment system (SPB), created by Law No. 12.214/01, and other entities of the SFN such as the BACEN and the CVM also regulate their operations. The members of the SPB are services or systems that:

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

10 As described in Article 2, IX, Law No. 9.385/76.
11 With an income of 10 million reais or less, as defined by Article 2, III, CVM Rule No. 588/17.
12 CVM Rule No. 588/17.
13 These organisations descriptions may be translated to ‘peer-to-peer lending company’ and ‘direct loans company’, respectively.
are referred to as financial market infrastructure; and
maintain payment arrangements and payment institutions, as provided by Law No. 12.865/13.

In order to guarantee the security of the transfer of resources, the regulation of the Brazilian payment system is quite solid and robust. In addition, the BACEN also manages and operates technological systems that guarantee interoperability among institutions, as with the System for the Transfer of Resources.

Regarding payment services, it is important to highlight the presence of the CIP – Interbank Payment Chamber – an entity composed of financial institutions, also a member of the SPB, which maintains technological solutions used by participants in payment settlement processes. In 2017, marketplaces of all kinds were determined to be part of payment arrangements, submitting themselves to the centralised settlement rules of their users' resources.

Moreover, 2018 was relevant to the means of payment market, as the BACEN introduced provisions expected to innovate and promote financial inclusion, as well as enabling a more competitive market.

By means of Resolution No. 4,707 and Circular No. 3,924, both of 19 December 2018, the BACEN governs the use of payment arrangement receivables as collateral for credit transactions. This should make loaning to smaller structures 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.

With Circular No. 3,925 of 20 December 2018, which amended the Annex to Circular No. 3.682 as of 4 November 2013, the BACEN addresses the provision of payment services within the framework of the arrangements of the Brazilian Payment System, establishing guidelines and standards these service providers need to abide by.

By means of Communiqué No. 32,927 of 21 December 2018, the BACEN recognises instant payments as valid and addresses the fundamental requirements for its environment within the Brazilian payment system regulatory framework. This enables 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 Constitution (and specific laws such the Supplementary Law No. 105/01) protects and assures the inviolability of banking secrecy, in most cases.

V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

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.\(^{14}\)

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 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,\(^ {15}\) it may be considered 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 foreign. The CVM also stated that investment funds cannot perform direct operations on crypto assets in Brazil. However, in September 2018, the regulator authorised indirect investment in cryptoactives 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 Bitcoin and other crypto assets. If the operation is for an amount higher than 35,000 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

\(^{14}\) The Central Bank conducted a research published in a paper named ‘Distributed ledger technical research in Central Bank of Brazil’, which can be found here: https://www.bcb.gov.br/htms/public/microcredito/Distributed_ledgerTechnicalResearchinCentralBankofBrazil.pdf.

\(^{15}\) 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 resultant from rendering of services, as described in Article 2, IX, Law No. 9.385/76.
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.

According to the latest version of FintechLab Radar (August 2018), the fintech market in Brazil can be divided into 10 major sectors: payments, financial management, credit and loans, investment, insurance, funding, data collection, cryptocurrencies and DLT, exchange and multiservices. It is also possible to highlight some new business models shown by specific companies that are very relevant in the market.

For this purpose, we may consider the credit card operator ‘Nubank’ as 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 startups in Latin America, becoming the latest 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.

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.

16 See Article 15, CVM Rule No. 505/11.
17 See Law No. 9.606/98, that regulates intellectual property for computer programs.
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.

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: the Brazilian General Data Protection Law (LGPD) that regulates the treatment of personal data in public and private sectors was enacted in August 2018. The Law was inspired by international guidelines, especially those provided by the European Union’s 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 law in Brazil that deals specifically with personal data protection.

The LGPD 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.
VIII YEAR IN REVIEW

From a data protection standpoint, the most important outcome was the enaction of the LGDP, which, although not currently in force, serves as a relevant guideline to personal data treatment in Brazil.

Additionally, in 2018, BACEN issued Resolution 4,658 and Circular Letter 3,909 that rule about cybersecurity policy and the requirements for contracting data processing, data storage and cloud computing services to be observed, respectively, by financial institutions and other institutions (including payment institutions) authorised to operate by BACEN. Financial and payment institutions subject to Resolution 4,658 and Circular Letter 3,909 must create and implement a cybersecurity policy that assures data confidentiality, integrity and availability that is compatible with the company’s size and characteristics, to the nature and complexity of the operations, as well as to the sensitivity of the data involved in the operations.

These new regulations state that financial and payment institutions should ensure that their policies, strategies and structures for risk management under the regulations in force, specifically regarding the decision criteria concerning to the outsourcing of services, contemplate the contracting of relevant processing services and storage of data and cloud computing, in Brazil or abroad. The regulations also bring specific requirements that should be observed in agreements involving data processing and cloud computing services.

Lastly, in 2018 BACEN published regulating acts that promoted innovation and the inclusion of new players to the market, including Resolution 4,656/18, which established new types of financial institutions: the direct credit company (SCD) and the peer to peer company (SEP). It presents standards (simpler than those applicable to other types of Brazilian financial institutions) to the incorporation, authorisation, operation, transfer of corporate control and corporate reorganisation of SCDs and SEPs.

The new rules are expected to facilitate the business environment of a large number of fintechs that used to operate as bank correspondents of other financial institutions.

IX OUTLOOK AND CONCLUSIONS

The main objectives of recent regulations were to guarantee better legal certainty, safety and confidence to the market. The authorities are showing cooperative behaviour, acting together in the production of norms that might affect the market. One example is the commentaries on cryptocurrencies and ICOs from the BACEN and CVM, issued on the same day and with similar viewpoints.

They are also combining efforts with the private sector, especially fintech players. Working together, the regulation may foster 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.
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;
b policing regulated activities with a view to reducing financial crime; and
c preventing market abuse.

---

1 Stephen Adams is a managing partner at Collas Crill.
Investment business

Generally, the statute with the most relevance is the Securities and Investment Business Act 2010 (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 Licenses 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, FUNDING AND PAYMENT SERVICES

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. In general, only open-ended funds are regulated. 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 an administrator, custodian, investment manager or auditor.

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, investment manager or auditor, 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 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 7

CAYMAN ISLANDS

Stephen Nelson

I OVERVIEW

With a long history of embracing financial innovation and providing a home for entrepreneurial technology companies, the Cayman Islands has seen organic development as a financial technology hub. The Islands’ regulator, Cayman Islands Monetary Authority (CIMA), has allowed the sector to flourish alongside the country’s existing legislative framework, and has pledged to introduce a legislative framework to encourage further development. The year 2018 saw a pullback from utility token (i.e., non securities) offerings and a move toward security token offerings (STOs) and stablecoin (or asset-backed coin) offerings (SCOs). In response to market forces and in order to follow industry best practices, in 2018, crypto-issuers and their offering agents expressed interest in, or sought, regulatory licensing. Similarly, many considered offering coins or tokens that held the backing of fixed assets such as metals and currency.

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 (2018 Revision), and its mission is to protect and enhance the reputation of the Cayman Islands as an international financial centre by fully utilising a team of highly skilled professionals and current technology, to carry out appropriate, effective and efficient supervision and regulation in accordance with relevant international standards and by maintaining a stable currency, including the prudent management of the currency reserve.

Anyone wishing to conduct banking, mutual 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 no 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 mutual funds business. We have set out the basic definitions below; however, 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 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 himself or herself out as willing, as principal, to buy, sell or subscribe for securities of the kind to which the transaction relates 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 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 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
- advice on the merits of his or her 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 EU connected funds;

_f_ marketing EU connected funds; 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 (2019 Revision) (SIBL), and includes, in general, shares, instruments creating or acknowledging indebtedness, instruments giving entitlement to securities, certificates representing securities, options, futures and contracts for differences. 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 (2010 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 Governor in Cabinet may specify by notice published in the Gazette; or
- the business of operating as an agent or franchise-holder of a business mentioned in (a) to (e) above.

**Currency exchange**

The third category of money services business is ‘currency exchange’, which is generally taken to mean the business of exchanging one currency for another. 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, regarding whether exchange services will 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.

**Mutual 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 (2018 Revision) (MFL).

The MFL applies to Cayman Islands entities, formed as collective investment schemes, that issue equities that are redeemable at the option of the holder. 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 as such will be required to comply with the MFL.

**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 (2018 Revision) 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. The definition of ‘the public’ does not include an offering to other exempted companies and exempted limited partnerships, and so, unless a fintech issuer is doing a focused offering into the Cayman Islands and to its general population, this obligation might not be triggered.
ii  Cross-border issues

The Cayman Islands does not 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, without limitation, the Local Companies (Control) Law (2015 Revision) (LCCL), the Trade and Business Licensing Law 2014, and to the extent any foreign workers are employed, the Immigration Law (2015 Revision).

However, as an alternative for placing operations in Cayman, there is Cayman Enterprise City, which permits incorporation and operation of a Special Economic Zone Company. Tech City Cayman has rapidly grown into a significant tech cluster housing some of the world’s leading blockchain and fintech companies.

Companies within Tech City Cayman Islands benefit 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.

III  DIGITAL IDENTITY AND ONBOARDING

The Electronic Transactions Law 2003 (ETL) bears review 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 effector 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 and electronic signatures are also expressly permitted. The ETL provides flexibility for transactional technologies without the requirement for further statute to be adopted. The ETL also provides a framework for the use of electronic signatures as a digital proof.

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 or MFL would apply.

ii  Collective investment schemes

As noted above, mutual funds are regulated by CIMA under the MFL. In general, only open-ended funds are regulated and must be registered with CIMA. All registered 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). Closed-ended funds and, by way of exception, open-ended funds with no more than 15 investors who, by

---

majority, can appoint or remove the operators of the fund (i.e., directors) 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.

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

**Registered mutual funds (MFL Section 4(3))**

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 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;
- a registration form (Form MF1) and letters of consent from the auditors and administrator;
- an affidavit from the directors of the fund;
- evidence of incorporation; and
- the prescribed registration fee and the initial administrative filing fee.

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 (MF Law section 4(1)(b))**

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))**

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.

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.
Directors of CIMA-regulated mutual 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).

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 CIMAConnect portal by providing details, including the name of the covered entity for which they are to act as director.

Regulated mutual 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 mutual funds (i.e., directors, trustees or general partners, as the case may be) also have a statutory obligation to notify CIMA:

- Of any change that materially affects the information in the prospectus or the application form of which they are aware, and to file an amended prospectus or amended Form MF1 within 21 days; and
- If the registered office or principal office of the fund has changed.

### 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

CIMA has not, to date, issued formal guidance on the issuance and distribution of cryptocurrencies and initial coin offerings (ICOs) and token offerings.

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, because it may result in the prior need to apply for and receive 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 to help avoid falling afoul of the LCCL, Companies, immigration laws or 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 does yet not have in force formal data protection legislation. However, the Data Protection Law 2017 (DPL) was passed by the Cayman Islands’ Legislative Assembly on 27 March 2017 and will come into effect in September 2019.

Generally, the DPL imposes strict regulations on entities handling personal data (data controllers), while simultaneously giving greater legal entitlements to persons whose data is being processed.

VII YEAR IN REVIEW

The Cayman Islands had a number of developments in 2018, including further industry utilisation of Cayman Islands foundation companies, bolstering of anti-money laundering measures, and introduction of international tax cooperation (economic substance) laws. As a purely observational aspect, we found that in 2018 most banking institutions (including those in the Cayman Islands) were reluctant to become involved with, and open banking relationships for, companies that planned to earn money from fintech or cryptocurrency-related businesses.

Cayman Islands foundation companies became a favourite in 2018 for issuers of SCOs and STOs. 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 – with a separate legal personality and a settled body of company laws. A multitude of issuers and related industry groups have gravitated toward foundation companies as an incredibly flexible tool for either the issuer vehicle or a corporate governance vehicle for acting on the e-vote of designated coin and token holders.

Recent changes to the Cayman Islands anti-money laundering legislation (the AML Regime), adopted to ensure that it more closely aligns with the revised Financial Action Task Force Recommendations, have:

a extended the scope of the AML Regime to apply to unregulated investment entities that are not registered with CIMA, including venture capital, private equity or other closed-ended investment funds, structured finance and investment related insurance entities; and

b enhanced the existing AML procedures, including a requirement for the appointment of certain designated officers (AMLCO, MLRO and Deputy MLRO), which now apply to all entities in scope of the AML Regime (such entities are termed ‘financial service providers’).

In most circumstances, token issuers and any funds investing in cryptoassets will be subject to the AML Register.

Notwithstanding that unregulated entities may not have previously specifically fallen within the scope of the AML Regime, international best practice has prompted most such entities to implement AML and combating of terrorist financing checks, policies and procedures (AML Policies). Unregulated entities will also likely have collected information
on their investors with respect to automatic exchange of information obligations under the Foreign Account Tax Compliance Act and the OECD’s Common Reporting Standard, which will assist with respect to the requirements under the AML Regime.

The appointment of a natural person as AMLCO, MLRO and Deputy MLRO for all existing funds was to have been effected in 2018, with notification for any CIMA-registered funds being made to CIMA.

The Cayman Islands government has published new legislation, the International Tax Co-operation (Economic Substance) Law 2018, which came into effect on 1 January 2019 (ESL). Further to this, the Economic Substance for Geographically Mobile Activities Guidance (the Guidance) and the International Tax Co-operation (Economic Substance) (Amendment of Schedule) Regulations 2019 (the Regulations) were published on 22 February 2019, providing additional detail and clarification in respect of the ESL.

The ESL sets out requirements applicable to in-scope Cayman Islands entities ( Relevant Entities) that carry on particular activities ( Relevant Activities), and that are not tax resident outside of the Cayman Islands, to demonstrate that such entities have ‘economic substance’ in the Cayman Islands.

The ESL has been passed as part of a move by the Cayman Islands to meet its commitments as a member of the OECD’s global Base Erosion and Profit Shifting Inclusive Framework and following consultation between the Cayman Islands government and the EU Code of Conduct Group (the Group), subsequent to assessment by the Group of the tax policies of a range of countries, including the Cayman Islands, and its inclusion in a list of jurisdictions (including the British Virgin Islands, Bermuda, Guernsey, Jersey and the Isle of Man) required to address the Group’s concerns in relation to economic substance.

The Cayman Islands Tax Information Authority will be responsible for compliance with the ESL, and it is expected that affected companies (being Cayman tax resident companies that are neither investment funds nor domestic companies) will notify and report directly to this entity starting in 2020.

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). Whether the reason is concern over AML/CFT aspects, or pressure from correspondent banking partners, or pressure from shareholders, there does appear to be a dearth of willing banking partners. Our clients 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.

VIII 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 may issue guidance in the future, which will be based on consultations with players in the blockchain industry. CIMA’s goal is to develop an effective and business-friendly fintech landscape, which also aligns with international standards as they continue to develop. At the same time, CIMA has stated that its primary concern with fintech offerings is the AML/
Cayman Islands

CFT-related aspect. 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, the Cayman Enterprise City and its successful Special Economic Zone Companies, the many fintech entrepreneurs that seek Cayman Islands as a jurisdiction for business look to be well served in the future.

---

Chapter 8

FRANCE

Eric Roturier

I OVERVIEW

In addition to the implementation of recent EU regulations (such as PSD 2 and GDPR), France has recently adopted new regulations relating to, in particular, crowdfunding and the issuance and transfer of certain non-listed securities through a DLT. France has recently adopted a framework for initial coin offerings (ICOs) and a framework for providers of crypto services.

Even though there is no ‘sandbox’ approach available in France (i.e., no new financial technologies can develop outside any regulation or benefit from a tailor-made regulatory regime), France is rather fintech-friendly.

The French banking regulator (ACPR) and the French financial markets regulator (AMF) launched a joint initiative in 2016 in order to accompany the fintech start-ups in their licensing process.

In addition, a Fintech forum has also been set up in order to foster dialogue between various stakeholders. These are public authorities such as the Ministry for the Economy and Finance, regulators such as the ACPR, the AMF, the data protection authority (CNIL) and the French National Cybersecurity Agency (ANSSI), companies and their lawyers. Meetings are generally held every quarter and address subjects from various perspectives.

---

1 Eric Roturier is a senior associate at Allen & Overy LLP. The author would like to thank Faustine Piechaud (an associate in the data protection department at Allen & Overy LLP in Paris) and Paul Vandecruix (an associate in the public law department at Allen & Overy LLP in Paris) for their assistance in the production of Section VII of this chapter and Hassan Benseghir (an intern in the international capital markets department at Allen & Overy LLP in Paris) for his assistance in this year’s update.


4 Pôle FinTech-Innovation at the ACPR and Division Fintech, innovation et compétitivité at the AMF.

5 Direction générale du Trésor.

6 The Commission nationale informatiques et libertés.

7 The Agence nationale de la sécurité des systèmes d’information.
II REGULATION

i Licensing and marketing

License

There is no special fintech licence in France; either the relevant service is regulated, and in that case the service provider must hold a licence, or the service is not regulated and in that case no licence is necessary.

In practice, most fintech companies provide regulated services and are regulated (either they apply for a licence in France or they benefit from an EU passport (see Section II.iv)).

In addition to the existing EU regulatory statuses (such as credit institutions, payment institutions, investment firms, management companies or insurance intermediaries) there are national statuses available in France to fintech companies provided that they meet the relevant requirements, such as independent financial advisers,8 intermediaries in banking transactions9 or intermediaries in crowdfunding activities.10

For instance, an automated digital advisory company may be regulated under different statuses depending on the type of clients it has and whether it provides other services. If the underlying product is a life insurance policy, the company can be regulated as an insurance intermediary (such as an insurance broker). If the company only provides investment advice, it can be regulated as an independent financial adviser or an investment firm, but if it provides other regulated investment services, it must be regulated as an investment firm. If the company can manage assets on behalf of the client, then it must be registered as a portfolio management company.

Marketing

The marketing of financial products or services is regulated. There are rules relating to the sale of the products themselves and specific rules where marketing is performed through solicitation activities. In addition and as a matter of principle, entities are generally prohibited from advertising without an appropriate licence.

ii Overview of the rules relating to the products

Offering transferable securities (such as shares and bonds) to the public in France is prohibited without an approved prospectus, unless an exemption applies. Specific rules apply to funds (UCITS or AIFs within the meaning of the EU directives).11 Other regulations may apply to the marketing of loans.

In addition, the EU Regulation PRIIPS12 applies to various structured products targeted at retail investors and it aims to increase the transparency and comparability of such products through the issue of a standardised short form disclosure document.

---

8 'Conseiller en investissements financiers'.
9 ‘Intermédiaire en opérations de banque et en services de paiement’.
10 'Conseiller en investissements participatifs' or 'Intermédiaire en financement participatif'.
iii  Solicitation rules

Solicitation activities are defined as any unsolicited contact (i.e., contact that has not been previously requested by the customers), by any means, with identified individuals or legal entities, where this contact is initiated and conducted with a view to obtaining customers’ consent to, in particular, the conclusion of a transaction on financial instruments, the conclusion of a banking transaction or an investment service or a related transaction or service. The scope of transactions and services caught by the solicitation rules is broad.

Solicitation activities will be considered as being carried out in France if they target French investors. The terms ‘contact by any means’ should be broadly interpreted, for example, including contact by email, telephone, internet and solicitation can be constituted even if this behaviour has not been repeated on a regular basis.

iv  Cross-border issues

Regulated activities can be passported from another jurisdiction into France provided that the activities are carried out by a company licensed in an EU (or an EEA) jurisdiction to provide such services, and comply with the formal passporting requirements (e.g., the company has to provide the home regulator with relevant information and unless the home or host regulator raises any objection, the company can be passported into France and start its activities).

Services passported in France can be provided either on the basis of the freedom of establishment (which means that the company needs to set up a branch in France) or of the freedom to provide services (i.e., no establishment in France).

The benefit of the EU passport is only available to those services that are subject to an EU directive or regulation.

If the company benefits from a ‘local’ licence in another EU jurisdiction, it cannot rely on any passporting regime and must be also licensed in France if it wants to provide services in France.

There could be exemptions for reverse enquiry situations (i.e., where contact has been instigated by a client to obtain information about a product or service).

III  DIGITAL IDENTITY AND ONBOARDING

On 5 January 2018, the Minister of Interior Affairs announced the launch of a unified digital identity process for all French citizens, foreign individuals legally resident in France and French companies, which would be effective in September 2019. This process would be integrated within the already existing digital platform of the French state and ‘France Connect’, a platform set up in June 2016 that offers a global system of identity management for online government services. The unified digital identity process would be designed so that it could be used for public services as well as for private entities.

Fully digitised onboarding of clients is possible provided that the relevant company performs the know-your-customer requirements to which it may be subject, and has set up a process for electronic identification (in particular accordance with the eIDAS Regulation).
In addition, a recent ordinance\textsuperscript{16} has clarified the rules relating to the digital transmission of pre-contractual and contractual information in the financial sector, which should also foster fully digitised onboarding of clients.

\section*{IV \hspace{1em} DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES}

As a preliminary remark, a fintech project may fall within the scope of the AIFM Directive if the relevant entity raises capital from a number of investors, with a view to investing it in accordance with a defined investment policy for the benefit of those investors, and is not a UCITS.\textsuperscript{17} The requirements are quite burdensome and fintech projects do not generally aim to fall into the definition of ‘alternative investment funds’. The French legal framework relating to, in particular, the banking monopoly and the scope of the public offer of securities, has recently been modified to allow crowdfunding activities.

\textbf{i} \hspace{1em} Crowdfunding

In France, to foster the development of crowdfunding in a secure environment for contributors (lenders, investors or donors), the public authorities have amended the regulations and created two new ‘light’ regulatory statuses for crowdfunding platforms: crowdfunding adviser and crowdfunding intermediary.

\textbf{ii} \hspace{1em} Crowdfunding adviser

A platform for crowdfunding via the subscription of financial securities issued by an unlisted company must be registered in the ORIAS register (i.e., a register for financial intermediaries, including insurance intermediaries, intermediaries in banking transactions, etc.) as a crowdfunding adviser (CIP). Their activities consist of providing investment advice, as their regular activity, on plain vanilla capital and debt securities (ordinary shares, fixed rate bonds and convertible bonds). The activities must be conducted by means of a progressive-access website, fulfilling the characteristics laid down by the AMF. In order to benefit from the exemption to the publication of a prospectus, the amount issued shall not exceed €2.5 million.\textsuperscript{18}

Such a platform may also opt for the status of investment services provider (ISP) providing investment advice services, in which case it must be licensed by the ACPR. Such platforms are regulated by the AMF alone in the case of CIPs and by the AMF and the ACPR jointly for ISPs.

\textbf{iii} \hspace{1em} Crowdfunding intermediary

If the website proposes to fund projects under the form of a loan with or without interest, the platform must be registered in the ORIAS register as a crowdfunding intermediary (IFP). We will focus in the rest of this paragraph on the intermediation of loans stipulated with or without interest, and granted to professionals (i.e., individuals acting in a professional

\begin{itemize}
\item \textsuperscript{16} Ordinance No. 2017-1433 of 4 October 2017 relating to the dematerialisation of contractual relationships in the financial sector.
\item \textsuperscript{17} Article L. 214-24-I of the Monetary and Financial Code.
\item \textsuperscript{18} Article D. 411-2 of the Monetary and Financial Code.
\end{itemize}
capacity or commercial companies) by individuals not acting for professional purposes.\(^\text{19}\) With a view to protecting lenders, the amount lent shall not exceed €2,000 per lender and per project where the loan is granted with interest and €5,000 where no interest is stipulated. The total amount borrowed shall not exceed €1 million.

IFPs are regulated by the ACPR.

According to publicly available statistics, France has around 100 crowdfunding platforms and is now the second largest crowdfunding market in Europe. Market consolidation is expected as a result of strong competition between the platforms.

iv Payment services

Since the implementation into French law in 2018 of EU Directive 2015/2366 on payment services in the internal market (PSD 2), two new payments services are now available: payment initiation and account information services.

V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

Blockchain technology is not regulated as such. However, the following two elements should be noted.

There has been a recent change to French securities law so that securities that are not traded via a central securities depository and a securities settlement system can be represented and transmitted using distributed ledger technology (DLT).

There are also two new frameworks: one for ICOs and another for providers of crypto services.

i Use of DLT for securities that are not traded via a central securities depository and a securities settlement system

A recent law\(^\text{20}\) granted the government powers to reform securities law so that securities that are not traded via a central depository and a security settlement system can be represented and transmitted using a DLT. An ordinance was published in November 2017\(^\text{21}\) following a public consultation. A decree was published in December 2019\(^\text{22}\) in order to specify the technical conditions applicable to this new regime.

In summary, an issuer of debt securities, commercial paper, units or shares of a fund or unlisted securities could decide to register such securities in a DLT, instead of a traditional securities account (which would facilitate the transmission of such securities).

The DLT would have to meet certain conditions, such as:

\begin{itemize}
\item[a] the owner of the securities must be able to access his or her statement of transactions;
\item[b] a business continuity plan must be in place; and
\item[c] the DLT must preserve the integrity of the transactions that are recorded.
\end{itemize}

\(^{19}\) Article L. 548-1 et seq. of the Monetary and Financial Code.


\(^{21}\) Ordinance No. 2017-1674 of 8 December 2017.

\(^{22}\) Decree No. 2018-1226 of 24 December 2018 on the use of an electronic recording device shared for the representation and transmission of securities and the issuance and sale of minibonds.
The decree has also clarified the provisions relating to the pledging of securities registered in a DLT.

This reform was preceded by a more limited one in 2016 (in terms of scope), as in April 2016 an ordinance authorised the issuance and transfer of certain types of promissory notes called 'minibons' in a DLT. Minibons can be issued through the website of a crowdfunding adviser or an ISP (see Section IV.ii).

ii New framework for ICOs

Following a consultation launched by the AMF on ICOs and numerous responses received from stakeholders, the new law 'Loi Pacte' aims at creating an optional regime for ICOs. Under the new optional regime, ICO originators could decide, on an optional basis, to request a marketing authorisation from the AMF, which would then issue its approval.

Tokens issued through an ICO would be defined as:

any intangible property representing, in digital form, one or more rights, which may be issued, registered, held or transferred through an electronic distributed ledger that identifies, directly or indirectly, the owner of such property.

Issuers who decide to obtain an approval from the AMF would have to submit to the AMF an information memorandum describing the ICO and any related marketing document.

The AMF would, in particular, ensure that the issuer is located in France and that adequate measures are in place to secure the rights of tokenholders.

If the tokens can be characterised as financial securities because of their characteristics, the legal framework for prospectuses should apply to the extent that the tokens are offered to the public.

iii New framework for providers of crypto services

The new law Loi Pacte also aims at creating a special legal regime for financial intermediaries that provide token-related services.

For the purposes of these provisions of the Loi Pacte, tokens are defined as:

any intangible property representing, in digital form, one or more rights, which may be issued, registered, held or transferred through an electronic distributed ledger that identifies, directly or indirectly, the owner of such property; or

any digital representation of a value which is not issued or guaranteed by a central bank or a public authority, which is not necessarily pegged to a currency which has legal tender and which does not have the legal status of a currency, but which is accepted by physical persons or non-natural persons as an means of exchange and which may be transferred, stored or exchanged electronically.

25 Action Plan for Business Growth and Transformation (PACTE), Article 26 bis (the law must nevertheless be enacted in order to enter into force).
Such definition includes tokens *stricto sensu*, which may be issued as part of an ICO but excludes securities tokens or more generally any token that has the characteristics of a financial instrument. It encompasses any cryptocurrency or any cryptoassets used as a means of exchange.

The new legal regime for token service providers would apply to any intermediary that provides the following services:

- the custody service of private cryptographic keys on behalf of third parties, in order to own, store or transfer tokens;
- the service of purchasing or selling tokens against fiat currency;
- the service of exchanging tokens against other tokens;
- the operation of a tokens trading venue; and
- the following services:
  - reception and transmission of orders on behalf of third parties;
  - portfolio management on behalf of third parties;
  - investment advice;
  - underwriting of tokens;
  - placing of tokens with a firm commitment basis; and
  - placing of tokens without a firm commitment basis.

A licence would be mandatory to provide services (a) and (b), namely, custody of private cryptographic keys and purchase, sale of tokens against fiat currency (licence granted by the AMF, in cooperation with the ACPR).

A licence would be optional to provide services (c) to (e) (licence granted by the AMF).

### IV AML rules

Following the implementation in France of the Fourth AML Directive 2015/849, platforms for the exchange of cryptocurrencies shall in particular be subject to anti-money laundering rules.

### VI OTHER NEW BUSINESS MODELS

A new regime applies as of 1 January 2018 to operators of online platforms (such as, for instance, marketplaces or websites comparing products). Operators of online platforms must provide customers with clear, accurate and transparent information and are therefore subject to various disclosure obligations. In this respect, they must specify the listing and delisting conditions of the contents, the criteria for the classification of the contents, as well as whether there is an equity-based relationship or a remuneration of their profit that might influence the classification or the listing of any of the contents.

---


27 Article L. 561-2-7° bis of the Monetary and Financial Code provides that ‘any person who, as a regular occupation, acts as counterparty or as an intermediary for the purchase or the sale of any digital instrument representing non-monetary units of value, which can be stored or transferred in order to purchase goods or services (but which does not represent a claim against any issuer)’ shall be subject to the AML rules.

28 Article 111-7 et seq. of the Consumer Code.
VII INTELLECTUAL PROPERTY AND DATA PROTECTION

i Intellectual property

In France, business models cannot be protected by intellectual property rights (copyright or patent),\(^{29}\), which means that fintech companies cannot protect their business models.

France has implemented the European Directive of 14 May 1991 on the legal protection of computer programs. Therefore, software can be protected by copyright, not by a patent. Software is automatically protected by copyright, provided that it meets the originality requirements. If the patentability of software is excluded as a matter of principle, such protection may be granted where the software constitutes ‘a step in an industrial process and/or in the operation of a system’.\(^{30}\)

Software created by one or more employees in the performance of their duties or following the instructions given by their employer belongs to the employer to which all the rights of authors are vested (unless the employment contract provides otherwise).

ii Data protection

The EU General Data Protection Regulation 2016/679 (GDPR) applies in particular to the processing of personal data if the fintech company is based in France or outside the EU and offer goods or services, or monitor the behaviour of data subjects in France.

As part of this new regulation, the fintech companies subject to the GDPR (either as ‘data controllers’ or as ‘data processors’) have to comply with a large number of obligations, which relate for example, but are not limited, to:

a. the principles applying to the processing of personal data, for example, lawfulness, fairness, transparency, purpose limitation, data minimisation and ‘privacy by design’, accuracy, storage limitation, security, confidentiality, etc.;

b. the ability of the controller to demonstrate compliance with such principles (accountability);

c. the obligation to identify a legal basis before the processing (special requirements apply to certain specific categories of data such as sensitive data); and

d. data subjects’ rights (e.g., transparency, the right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object to a processing).

The application of the GDPR has compelled many fintech companies to launch comprehensive GDPR compliance programmes, including data mapping efforts, gap analysis and implementation programmes (e.g., by way of amendment of current internal processes, contracts, software’s technical characteristics).

GDPR also provides for rules relating to profiling activities.\(^{31}\) Profiling involves three elements:

a. it has to be an automated form of processing;

\(^{29}\) In accordance with Article L. 611-10 of the Intellectual Property Code.


\(^{31}\) Article 4(4) of GDPR defines ‘profiling’ as ‘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’.
it has to be carried out on personal data; and
the objective of profiling must be to evaluate aspects about an individual.

Under GDPR, fully automated individual decision-making, including profiling, that has a legal or similarly significant effect is prohibited unless limited exceptions apply. Automated processing is deemed to significantly affect an individual in the following scenarios: online advertising solely based on automatic processing means where the individual being targeted is vulnerable (e.g., children, minority group) or differential pricing where higher prices effectively bar individuals from certain goods or services.

Fintech companies must ensure, as part of their GDPR compliance programmes, that suitable measures are in place to safeguard the rights and interests of individuals.

VIII YEAR IN REVIEW

The Fintech Innovation Hub, launched by the ACPR, has addressed one of the most significant barriers to entry for fintech companies, which lies in the spread of and knowledge about financial regulation ‘which may sometimes be very complex, especially for entrepreneurs that did not work in the financial sector before’. Since the launch of the Hub in June 2016, more than 200 financial players have been offered a meeting or a call with the Hub. Since the ACPR Hub welcomes fintech at the early stages, it is able to identify promptly evolving market practices and new business models.

Since the beginning of the UNICORN programme launched by the AMF for ICOs (involving the support and analysis of ICOs), the AMF has met more than 25 undertakings. The AMF’s discussions have shown that tokens issued as part of the examined ICOs vary considerably from project to project. Most of the tokens were utility tokens, giving the holder the right to use the technology or services distributed by the ICO promoter.

With regard to payment services providers, the introduction of two newly regulated services (payment initiation and account information) by PSD 2 requires access for new actors (third-party providers) to the accounts held by other PSPs (such as traditional credit institutions). This means that existing credit institutions would have to open access to their clients’ data. This should foster open banking. In France, these new actors (which were unregulated before PSD 2) are quite active and can provide other services to their customers such as investment advice, accounting, etc.).

32 Articles 21 and 22 of GDPR.
33 Joint answer from Banque de France and ACPR to the European Commission’s Public consultation on Fintech: a more competitive and innovative European financial sector: https://acpr.banque-france.fr/sites/default/files/medias/documents/20170615_reponse_consultation_europe_0.pdf.
34 According to Didier Warzée, member of the ACPR’s Fintech Innovation Hub.
35 Universal Node to ICO’s Research & Network.
IX OUTLOOK AND CONCLUSIONS

In terms of regulatory developments for the following year, there is particular focus on the implementation of both PSD 2 and GDPR, which will give more rights to consumers. All participants (both existing financial institutions and new fintech companies) will have to comply with the new data protection rules.

It remains to be seen whether the reform of the securities law will really be a game changer for non-listed securities (in particular for the distribution of units or shares of funds through a DLT).

There are two new frameworks: one for ICOs, another for providers of crypto-services, as France is keen to attract and develop such activities and better regulate them.

In terms of market activity, many fintech companies may decide not to compete directly with existing players but to cooperate with them. The financial sector is quite mature in France and the market shares of fintech companies is rather limited for the moment. The cooperation may take the form of partnerships or equity stakes. In any case, all existing actors in the banking, asset management or insurance sectors acknowledge the impact of digitalisation on their activities and the need to innovate.
I OVERVIEW

Since the publication of the first edition of The Financial Technology Law Review in 2018, the German fintech market has continued to evolve, even though the expansion of the fintech market in Germany has slowed down compared to the previous years. Fintech-related topics are still frequently and intensively being discussed in Germany not only by participants in the financial sector but also by politicians and regulatory authorities. In recent months, particularly the question whether cryptocurrencies like bitcoin qualify as financial instruments and whether the present legal framework gives sufficient leeway for the application of blockchain-based business models have been the subject matter of such discussions.

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 include 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 to foster 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.

1 Jens H Kunz is a partner at Noerr LLP.
3 See Gregor Dorfleitner et al., ‘FinTech-Markt in Deutschland’, 17 October 2016, a study assigned by the Federal Ministry of Economics.
4 See German Federal Ministry of Finance (Bundesministerium der Finanzen), www.bundesfinanzministerium.de/Content/DE/Pressemittelungen/Finanzpolitik/2017/03/2017-03-22-pm-fintech.html (15 February 2019).
6 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 (15 February 2019).
Germany

security. So far, however, the various initiatives have not resulted in any special fintech legislation, save for a relief in the regulation for crowdfunding platforms that is of particular relevance for peer-to-peer lending platforms as introduced by fintech businesses.8

Generally, German legislators and BaFin apply the principle of ‘same business, same risk, same regulation’. This includes that neither the legislators 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. In this connection, 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 €100,000.9 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. 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 seems rather conservative when the traditional regulatory standards, which stem from the era of pre-digitalisation, 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 the indicators for future legislative changes to foster technical innovation, 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 ‘same business, same risk, same rules’ approach. The entire array of licences and marketing restrictions may therefore become relevant for fintech business models.

8 Section 2a of the Asset Investment Act (Vermögensanlagengesetz, VermAnlG), which exempts such platforms from certain requirements as, for instance, the obligation to publish a prospectus provided that certain threshold amounts have not been crossed.
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 investment services within the meaning of Section 1(1a)(2) KWG;
- **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, 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 get 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.

It would exceed the given framework to elaborate on the licence requirements for each fintech relevant business model. However, the general rule that the necessary type of licence depends on the specific services to be offered can be illustrated by reference to the robo-advice business models which 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 follow from the Act against Unfair Competition (UWG) but are also included in some of the statutory provisions for financial services. 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

10 More comprehensive capital and other requirements apply if the robo-adviser is entitled to hold the assets and funds of its clients.
12 Section 64(4) Securities Trading Act (WpHG).
13 Section 32(1) of the KWG within the meaning of Section 1 (1a)(2)(3) KWG.
14 Section 63(6) WpHG, Section 302 KAGB and Section 23 KWG.
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.

ii 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.15

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 German customers among users of different nationalities.16 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

15 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/mi_050401_grenzueberschreitend_en.html (13 March 2019).

16 Cf. Federal Administrative Court (Bundesverwaltungsgericht), decision of 22 April 2009, Az. 8 C 2/09, juris margin: 41.
supervisory authority of its intent to offer the regulated services also in Germany. 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 well-regulated withdrawal from the EU, including transitional periods, fintechs based in the United Kingdom providing regulated services will not have the opportunity any more to offer such services on a cross-border basis to customers in EEA Member States under the EU-passport regime.

Another possibility for fintech companies to access the German market without being subject to a licensing 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.

III DIGITAL IDENTITY

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).

Regarding the onboarding process as required under the statutory anti-money laundering and counterterrorism rules, the Anti-Money Laundering Code (GwG), which was revised in 2017, confirmed the possibility of video identification ensuring onboarding without media discontinuity, which is often particularly important for fintech business models. The requirements for such video identification are, however, rather strict. Given that BaFin confirmed the applicability of these standards in its guidance on the interpretation of the GwG published in December 2018, an alleviation of the requirements is not to be expected.

IV DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES

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.

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.\(^{20}\) 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.\(^ {21}\) The key concern relates to possible licensing requirements. In particular, the licensing requirement for lending business must be considered.\(^ {22}\) 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.\(^ {23}\) 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


\(^{22}\) Section 32(1) KWG in connection with Section 1(1)(2)(2) KWG.

\(^{23}\) Section 32(1) KWG in connection with Section 1(1)(2)(1) KWG.
business. In these models, the fronting bank extends the loans to the borrowers, and the bank refinances 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.

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. 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.

**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. BKG). These rules are based on EU law and should in general not differ in the EU Member States.

---

24 Section 1(1a)(2)(9) KWG.
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 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.25

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, is expected to offer new business opportunities especially for nimble fintech companies. The reason for this expectation is that account information services and payment initiation services as new payment services have been 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).

This opportunity, however, comes with additional regulatory burden. 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.

---

25 See in more detail at Section V.ii.
V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

i Cryptocurrencies

Cryptocurrencies such as bitcoin undoubtedly constitute a challenge for the German law from regulatory, civil law and tax perspectives. This is because legislators have not yet enacted any special rules for the legal treatment of cryptocurrencies.

In the absence of specific regulations dealing with cryptocurrencies, BaFin made a first step towards the regulation of cryptocurrencies through a broad interpretation of the term ‘financial instrument’ within the meaning of the KWG. According to BaFin, cryptocurrencies such as bitcoin qualify as ‘units of account’ within the meaning of Section 1(11) No. 7 alt. 2 KWG and therefore as financial instruments. This is an important determination, as it means that services related to cryptocurrencies that are provided commercially or on a commercial scale may be subject to a licensing requirement. However, this view of BaFin was recently challenged by a ruling of a higher regional court in criminal proceedings. The court held that bitcoins do not constitute ‘units of account’ within the meaning of the KWG and that the sale of bitcoins are therefore not subject to a licensing requirement the non-compliance of which would result in committing a criminal offence. This ruling sparked controversial discussions regarding whether BaFin may adhere to its qualification of bitcoin and similar cryptocurrencies as financial instruments. As a matter of practice, however, the German federal government provided the answer to this question by clarifying that the court ruling does not concern the administrative practice of BaFin. Against this background, one should not rely on said court ruling but take into account BaFin’s view on bitcoin and similar cryptocurrencies in assessing the legal risks related to relevant business models. For instance, 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. Further, brokering cryptocurrencies might constitute investment brokerage, whereas advising on the purchase or sale of cryptocurrencies might be considered investment advice. 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 might, therefore, be subject to a licensing requirement.

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.

26 Higher Regional Court of Berlin (Kammergericht Berlin), decision of 25 September 2018 – (4) 161 Ss. 28/18 (35/18).
27 Printed Paper of the German Bundestag 19/6034.
28 Section 1(1)(2)(4) KWG.
29 Section 1(1a)(2)(1) KWG.
30 Section 1(1a)(2)(1a) KWG.
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.

Interestingly, the usually complex tax analysis has at least partly already been clarified for cryptocurrencies through a decision by the European Court of Justice (CJEU).\textsuperscript{32}

According to the principles of this decision that were incorporated into German tax law,\textsuperscript{33} 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 bitcoins 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 bitcoins 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{34} 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{35}

\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{36}
\end{itemize}

\textsuperscript{32} Cf. European Court of Justice, decision of 22 October 2015, C-264/14, V, Hedqvist.


\textsuperscript{34} Kirsch / von Wieding, Bilanzierung von Bitcoin nach HGB, BB 2017, 2731, 2734.

\textsuperscript{35} Kirsch / von Wieding, Bilanzierung von Bitcoin nach HGB, BB 2017, 2731, 2734.

\textsuperscript{36} Blockchain Bundesverband, Finance Working Group, Statement on token regulation with a focus on token sales (undated), p. 3.
This rough categorisation – which corresponds to the general approach pursued by BaFin – illustrates that tokens may differ significantly. Consequently, each ICO must be thoroughly analysed with respect to its regulatory and capital market requirements. BaFin determines the applicability of the applicable 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.37

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, would, as a general rule, require licensing by BaFin.38

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.39

iii Money laundering rules

Tokens and cryptocurrencies in general are perceived as highly susceptible to money laundering and terrorism financing. So far, however, special legislation has not been adopted in Germany to address such risks relating to ICOs and cryptocurrencies.

Yet, this does not mean that the existing German anti-money laundering and counterterrorism rules do not apply to cryptocurrencies and ICOs. Owing to the broad interpretation of the term ‘financial instrument’, cryptocurrency and ICO service providers may be subject to a licence requirement under the KWG. In this case they must, in their

38 See in more detail at Section V.i.
capacity as institutions, adhere to the duties set out in the Anti-Money Laundering Act (GwG). This includes having to conduct adequate customer due diligence and, as appropriate, notifying the Financial Intelligence Unit of any suspect transactions.

The more interesting question is whether also 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. 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).

To summarise, in Germany the statutory AML-rules may become relevant in the context of transactions with cryptocurrencies and ICOs, but there is still some ambiguity. More clarity will be achieved by the implementation of the stricter rules provided for in the 5th EU-AML Directive, which became effective on 9 July 2018. The 5th EU-AML Directive extends the scope of the AML requirements to operators of virtual currency platforms, which shall have the same customer identification obligations as banks. The new rules will be transposed into German law by 10 January 2019.

VIOTHER 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.

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.41

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 evolved.

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.\(^ {42} \) 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 partly they offer white-label solutions, namely they may seek to cooperate with other fintech companies that need licensed banks for their business 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).\(^ {43} \)

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.\(^ {44} \) The capacity of being the originator is strictly connected to a natural person and may therefore not be transferred.\(^ {45} \) 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.\(^ {46} \) 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.\(^ {47} \)

ii Data protection

Generally speaking, data protection is governed by the Law on Telemedia (TMG) and 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,

\(^ {42} \) BGH, decision of 9 December.1975 - VI ZR 157/73, ‘Warentest II’.
\(^ {43} \) Cf. Bullinger, Wandtke/Bullinger, Praxiskommentar zum Urheberrecht, edition 4, Section 2 rec. 24.
\(^ {44} \) Cf. Bullinger, Wandtke/Bullinger, Praxiskommentar zum Urheberrecht, edition 4, Section 7 rec. 3.
\(^ {45} \) Cf. Benkard, Patentgesetz, edition 11, Section 15 rec. 5.
\(^ {46} \) Cf. Wandtke, Wandtke/Bullinger, Praxiskommentar zum Urheberrecht edition 4, Section 43 rec. 50.
\(^ {47} \) Cf. Rother, Rechte des Arbeitgebers/Dienstherrn am geistigen Eigentum, GRUR Int. 2004, 235, 237.
changing the fundamental principles of German data protection law. The GDPR and the TMG intend to prevent the collection and use of data related to individuals unless it is duly necessary to do so (Section 12(1) of the TMG, 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.48

Collection and processing of data related to individuals is only permitted if it is explicitly allowed by law or if the data subject consents (Section 12(1) TMG; Article 6(1) GDPR). Sections 14 and 15 of the TMG contain such allowances, if data are necessary to design a contract concerning the use of telemedia, to grant the user access to services or to charge those services properly. Furthermore, the user can declare his or her consent electronically (Section 12(2) of the TMG). 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 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, the fintech market in Germany continues to demonstrate growing maturity. This, and that business models of German fintech companies are able to implement commercially viable business models, may be 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 fintechs but also by developing their own digital offerings. This might explain why investment volumes and the number of noteworthy deals in 2018 did not reach the level of previous years.

ICOs and cryptocurrencies continue to be among the dominant topics in the fintech sector. For the time being, there is still a lack of specific regulation, which might be one of the explanations why risks such as high volatility, fraudulent business models and a lack of adequate customer information often accompany investments in ICOs and cryptocurrencies.

---

48 CJEU, decision of 19 October 2016 – C-582/14.
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 that provide more guidance on the regulatory treatment of ICOs and cryptocurrencies. 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.

The implementation of PSD II has opened the door for nimble fintech companies taking advantage of open banking possibilities by offering account information and payment initiation services.

IX OUTLOOK AND CONCLUSIONS

Given the numerous initiatives at an international, EU and national level dealing with the regulatory challenges of fintech, specific regulation has to be expected. With regard to cryptocurrencies and ICOs this is likely to result in tighter or at least clearer statutory requirements. The 5th EU-AML Directive illustrates this trend by implementing customer identification obligations for virtual currency platforms. 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 artificial intelligence.
Chapter 10

GUERNSEY

Wayne Atkinson

I OVERVIEW

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 Grill 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: 5

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 20,000 investors shared among 213 (largely investment fund) clients and around 700 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, FUNDING AND PAYMENT SERVICES

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 and 
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 PoI Law.
7 Paragraph 1(a) of Schedule 1 to the PoI Law.
8 Paragraphs 1(1)(b) and 1(1)(c)(ii) of Schedule 1 to the PoI Law.
9 Paragraph 1(c)(ii) of Schedule 1 to the PoI 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 AND INITIAL COIN OFFERINGS

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, the extent to which the POI Law licensing obligations will apply in the cryptocurrencies or

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.
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 2000.15 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:

\[a\] 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;
\[b\] contracts may be formed by the interaction of electronic agents (without input from natural persons); and
\[c\] contracts may be formed by the interaction of an electronic agent and a natural person.

An ‘electronic agent’ is defined in The Electronic Transactions (Guernsey) Law 2000 as:

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

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.

15 The Electronic Transactions (Guernsey) Law 2000.
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 11

ITALY

Giuseppe Rumi, Federico Vezzani and Tommaso Faelli

I OVERVIEW

Fintech is radically innovating the way financial services are designed and offered. 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 and artificial intelligence).

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. In this regard, 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 potential risks that might emerge regarding, among other things, consumer protection. 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.

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 context, 2019 is expected to witness the IPO of Nexi SpA, one of the Europe’s biggest players in the payment services market. Other developments are also taking place in the credit sector, securities trading and risk management.

The Italian government and competent authorities are establishing an increasingly fintech-friendly environment. More specifically, in 2017:

a the Bank of Italy (BoI) demonstrated its forward-looking approach by launching a fintech hub on its website to support innovation processes in the regulatory arena;2 and

b the Italian Companies and Stock Exchange Commission (Consob) launched several initiatives, including research programmes concerning robo-advice, blockchain and,
more generally, the relationship between fintech businesses and traditional financial activities. The initiatives are aimed at understanding more about the aspects that can influence the financial system and at regulating the fintech phenomenon.  

In March 2018, the Ministry of Economy and Finance (MEF) established a coordination committee in response to a memorandum of understanding between the MEF, the BoI, Consob and other national authorities. The Committee’s purposes are:

- to encourage the introduction of innovative services and models in the financial and insurance sectors;
- to monitor fintech developments; and
- to develop general principles applicable to fintech and propose appropriate amendments to the current legal framework.  

Furthermore, the increasing attention to cyberspace and technological developments brought the Italian government to recently issue innovative regulations governing blockchain, cryptocurrencies and crowdfunding (see Sections IV and V); and establish specific funds to support fintech developments and encourage investments in areas connected to artificial intelligence, blockchain, internet of things and cybersecurity.

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

- 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);
- 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
- tax credit on research and development activities, according to which companies can benefit from a tax credit equal to 50 per cent (or 25 per cent depending on the kind of expense) of the incremental R&D expenses.

II REGULATION

i Licensing and marketing

Currently, the Italian regulatory framework provides no definition of ‘fintech’ business. Therefore, 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 portals’ 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 out them. Therefore, fintech firms that perform banking activities, investment services and asset management activities (including automated digital advisory (robo-advice) and digital asset and wealth management services), payment services or insurance activities are subject

---

3 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.

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, 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, 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).

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.

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

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).

An innovative remote video-identification procedure to meet customer due diligence requirements for AML purposes is expected to be specifically regulated in the near future following the BoI’s draft regulations published for public consultation in April 2018.
IV DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES

i Crowdfunding

Italy was one of the first countries in Europe to introduce specific legislation governing equity crowdfunding, which is laid down in the Italian Financial Act\textsuperscript{12} and Consob Regulation No. 18592 of 26 June 2013.\textsuperscript{13} Under this legislation, the management of equity crowdfunding portals is limited to:

- investment firms and banks authorised to provide investment services, which are considered ‘\textit{de facto} managers’ and require no specific licence; and
- portal managers other than those under point (a), which need to be duly authorised and enrolled on a special register managed by Consob.

Equity crowdfunding portals may only be used to offer to the public financial instruments that are issued by small and medium enterprises (SMEs), collective investment schemes and social enterprises.

In this respect, Law No. 145/2018 (the 2018 Budget Law) recently introduced the possibility to also offer debt instruments, provided that this is carried out through a separate area of the portals and these instruments are addressed only to professional investors and other categories of investors identified by Consob. To date, the relevant implementing regulation of the 2018 Budget Law is yet to be published.

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 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{14}

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’:

- managers of the 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
- borrowers: if they acquire funds from:
  - individual lenders (following personalised negotiations) that are supported by the platform manager only to enable the execution of the agreement; or
  - entities subject to prudential supervision.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{12} As amended by Law Decree No. 179/2012, converted into Law No. 221/2012.
\item \textsuperscript{13} www.consob.it/documents/46180/46181/reg_consob_2013_18592_in_vig_2018.pdf/37067552-9179-489a-b18c-05fc30545d7e. Consob also has the following web page with all the relevant crowdfunding information: www.consob.it/web/investor-education/crowdfunding#c2.
\item \textsuperscript{14} https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/raccolta-risparmio-soggetti-diversi/index.html.
\end{itemize}
\end{footnotesize}
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. 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.

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. Italian implementing rules introduced a specific regulation governing third-party providers (TPPs), which are typically payment initiation service providers (PISPs) and account information service providers (AISPs). PISPs and AISPs 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, as the BoI recently pointed out, 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.

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.

15 See Article 106 of the Italian Banking Act.
16 See Article 4, Paragraph 1, of Law No. 130 of 30 April 1999 and Article 58 of the Italian Banking Act.
V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

In February 2019, Law No. 12/2019\textsuperscript{18} 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. To date, the implementing technical standards providing the DLT requirements that ensure these transactions have legal effect are yet to be published. However, the 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\textsuperscript{19} and the signing of the Southern European Countries Ministerial Declaration on Distributed Ledger Technologies in December 2018.\textsuperscript{20}

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). This defines virtual currencies as ‘the digital representation of value, not issued 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 and that is transferred, stored and traded through electronic devices’.\textsuperscript{21}

The AML Decree expressly defines also virtual currency service providers as:

\[
\text{each natural or legal person providing to the third parties, in a professional manner, useful services to use, exchange, store the virtual currencies or to convert them in fiat currencies.}\textsuperscript{22}
\]

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).\textsuperscript{23} Once this Decree enters into force, virtual currency service providers will be required to:

\begin{enumerate}
  \item notify the MEF of the commencement of their activities; and
  \item enrol with a special section of the currency exchangers’ register.
\end{enumerate}

Failure to comply with the notification duty under point (a) may result in the application of specific administrative penalties.

Additionally, even before the AMLD V’s entry into force, Legislative Decree No. 90/2017 extended 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 exchange services between fiat currencies (i.e., currencies having legal tender) and virtual currencies (exchanges). This extension –

\textsuperscript{18} That converted into law, with amendments, Decree Law 14 December 2018, No. 135.
\textsuperscript{21} See Article 1, Paragraph 2, let. qq) of Legislative Decree No. 231 of 21 November 2007, as amended by Legislative Decree No. 90 of 25 May 2017.
\textsuperscript{22} See Article 1, Paragraph 2, let. ff) of the AML Decree.
\textsuperscript{23} 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 in general the application of AML duties to parties operating in the cryptocurrencies and tokens field – have raised concerns, at both European and national level, owing to the volatility of virtual currencies.24

The above definition of virtual currencies first appeared in a communication published by the BoI in 2015,25 which contained clarifications of the characteristics of virtual currencies; and, in line with the European Banking Authority (EBA),26 a warning about the use of these currencies, as they could result in a breach of Italian regulations with the risk of criminal penalties.27

In 2018, the BoI issued another communication declaring its adherence to the European Supervisory Authorities (ESAs) warning on virtual currencies28 and discouraging Italian banks, other supervised entities, and consumers from buying or selling virtual currencies following several scandals involving cryptocurrencies.29 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 recently published a consumer warning regarding the cryptocurrencies-related risks.30 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)31 without the necessary prior authorisation.32 Furthermore, on 19 March 2019, Consob published for consultation a discussion paper on the possibility to regulate cryptoassets and ICOs.

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.

24 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).
26 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.
27 See Articles 130 (abusive activity of collection of savings), 131 (abusive banking activity) and 131 ter (abusive provision of payment services) of the Italian Banking Act, and Article 166 (abusive provision of investment services) of the Italian Financial Act.
29 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.
30 http://www.consob.it/documents/10194/0/Articolo+susu+rischi+criptovalute/10402b10-bc3b-4500-a0d4-81ece9a2d2b3.
31 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.
32 See, for example, Consob Resolutions No. 20693 of 14 November 2018 and No. 20741 of 12 December 2018, whereby Consob suspended an offer of tokens and an offer of virtual currencies under Article 99 of the Italian Financial Act.
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:

- 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
- companies are subject to tax under the general corporation tax regime for profits and losses (currently, corporate income tax rate is 24 per cent).

With reference to VAT, the Italian tax authority is aligned with the position of the European Court of Justice – the *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.

**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:

> an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code.33

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 likely to create partnerships with existing fintech companies. This would allow them 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.

In this context, social-lending and digital lending platforms represent a new funding model for individuals and SMEs that sometimes face difficulties in accessing traditional bank funding. In these cases, the transfers between lenders and borrowers are carried out through a digital platform, thereby reducing the costs associated with the traditional financial intermediation of banks and increasing the remuneration deriving from lending activities (see Section IV).

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 Act 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.

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 EU Directive (EU) 2016/1148 concerning measures for a high common level of security for network and information systems across the European Union. In addition, in its Strategic Plan 2017–2019, the BoI included initiatives to improve the security and business continuity of the Italian financial sector by implementing a cyber-resilience strategy for Italy’s financial market infrastructure. In line with the Strategic Plan, the Bank of Italy and the

---

34 See, for example, Buddybank (the digital bank powered by Unicredit), CheBanca! (part of Mediobanca’s group) and Widiba (part of MPS group).
36 See Article 67 ter of the Italian Financial Act.
Italian Banking Association (ABI) have sponsored the establishment of the Italian Financial Cybersecurity unit, 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.38

With regard 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,39 as also provided by the Insurance Distribution Directive.40 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.

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:

- inventions by the employee in performing his or her work duties: the employer is the owner of IP rights over the employee’s inventions;
- 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;

38 https://www.certfin.it/.
39 See Articles 106 and 108 of Legislative Decree No. 209 of 7 September 2005.
40 See Article 2, Paragraph 1, No. 1 of Directive 2016/97/EU.
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.

VIII YEAR IN REVIEW

As highlighted in the results of a survey launched by the BoI and published at the beginning of 2018, financial sector players’ interest in fintech is growing. The main sectors to have seen investments are technologies that facilitate the conclusion of cross-border contracts or transactions, supporting technologies, payment services, robo-advisers, crowdfunding, cloud computing, cybersecurity, cryptocurrencies, DLT and smart contracts. The ultimate aim behind investment in these sectors is to gradually dematerialise and align their internal regulatory frameworks with rules defined at a national and supranational level.

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 banking operators are responding with the following strategies to adapt their current market demands:

a. development of platform services;
b. acquisitions or alliances with fintech companies; and
c. 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 is still limited from a quantitative point of view, with the focus for now being mainly on payment services, ‘transversal’ technologies and crowdfunding. The BoI is about to launch a new financial sector survey to record any new fintech initiatives and projects.

Against this backdrop, the Italian regulatory framework has undergone significant reforms that have impacted the fintech sector. More specifically, throughout 2018 and 2019, 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 Italian Financial Act, Consob’s Intermediaries Regulation and Consob’s Regulation No. 20249 of 28 December 2017 were amended and supplemented to implement MiFID II;
b. the Italian Banking Act and the BoI’s supervisory instruction to payment institutions was placed under consultation from July to September 2018 to implement PSD II (see Section IV);
c. the 2018 Budget Law introduced the possibility for crowdfunding portals to offer also debt instruments, and Consob’s Regulation No. 18592 of 26 June 2013 was amended and supplemented to implement MiFID II (see Section IV);
d. Law No. 12/2019 introduced the definitions of distributed ledger technology and smart contracts (see Section V); and
e. the BoI’s provisions on customer due diligence duties for AML purposes were placed under consultation from April to June 2018 (see Sections III and V).

At European level, in March 2018, the European Commission launched a fintech action plan, aimed at, among other things:

a. supporting innovative business models;
b. encouraging the uptake of new technologies in the financial sector;
c. increasing cybersecurity in the financial market; and
d. improving the integrity of the financial market.42

According to the action plan, the European Commission will, among other things:

a. host an EU fintech laboratory where European and national authorities will engage with tech providers in a neutral, non-commercial space;
b. present a blueprint with best practices on regulatory sandboxes, based on guidance from ESAs; and

42 See the European Commission’s Action Plan published on 8 March 2018.
report on the challenges and opportunities of cryptoassets later in 2018 in the framework of its Blockchain Observatory and Forum, which was launched in February 2018 for a two-year period.

Additionally, the EBA published a fintech roadmap setting out its priorities for 2018 and 2019, including the establishment of a FinTech Knowledge Hub to enhance knowledge sharing and foster technological neutrality in regulatory and supervisory approaches.43

IX OUTLOOK AND CONCLUSIONS

Technology-enabled innovation in financial services is fast developing and offers numerous advantages. Indeed, fintech has the potential to:

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 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. Although the benefits of technological change could take some time to fully materialise, innovation is contributing to cost savings, reduced information asymmetry, increased efficiency and competition, and wider access to financial services.

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 150 fintech companies are based in Italy, and this number continues to grow. Crowdfunding is the largest sub-sector of the fintech industry, with 51 active companies, 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 recently started seeing fintech as a way to innovate their everyday business, and plan investments that take advantage of fintech solutions.

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. In this regard, it can reasonably be expected that many new initiatives will result from the action plan on fintech launched by the European Commission in March 2018 (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.

Even though financial services are still predominantly distributed through traditional channels, technology-enabled innovation in financial services is fast developing and offers numerous advantages as technology dramatically reduces the costs of transmitting, processing and storing data, pushing towards new forms of financial intermediation.
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.

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. In fact, recent legislation in response to fintech (such as amendments to the Banking Act) shows government policy aims to promote the development of fintech, with minimal regulations for consumer protection, while the allocation of responsibilities between start-ups and financial institutions is left as a matter to be governed by private contracts or industry standards.

On the other hand, early 2018 revealed the fragility of cryptocurrency businesses where operators’ management systems have not adequately caught up with rapid business growth, so the government was forced to resort to stronger regulations. Specific examples include the Financial Services Agency’s (FSA) re-inspection of the operations of cryptocurrency exchange operators, and progression towards revising the regulatory framework to meet the upsurge of initial coin offerings (ICOs). The FSA published a study group’s report at the end of 2018, and submitted bills to strengthen existing regulations governing cryptocurrency exchange operators to the Diet in March 2019, and to introduce new regulations for cryptocurrency custody services and ICOs.

As a general reference resources 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

---

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/.
II REGULATION

i Licensing and marketing

Regulatory overview

Like other jurisdictions, the legal framework of financial regulations in Japan is 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 as on money laundering regulations and personal information protection.

<table>
<thead>
<tr>
<th>Products/services layer</th>
<th>Banking services</th>
<th>Prepaid payment instruments; credit; credit-purchasing intermediaries</th>
<th>Fund transfer services</th>
<th>Crypto-currency exchanges</th>
<th>Moneymaking businesses</th>
<th>Type I/II financial instruments businesses; investment management services</th>
<th>Insurance businesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales/marketing layer</td>
<td>Bank agency services; electronic settlement agency services</td>
<td>Crypto-currency exchanges</td>
<td>Moneymaking businesses</td>
<td>Financial instruments brokerages</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure layer</td>
<td>Moneymaking 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, cryptocurrency exchange operators, 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 is performed by the Ministry of Economy, Trade and Industry.

ii Banking

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.

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.

**Cryptocurrency exchanges**

In 2016, the Payment Services Act (PSA) was amended to include new regulations on cryptocurrency exchange businesses. Buying and selling cryptocurrencies or exchanging them with other cryptocurrencies is regarded as cryptocurrency exchange business, for which cryptocurrency exchange operators must obtain registration from the local finance bureau. The revision of these regulations is now under discussion. See Section V.

**Lending**

To provide moneylending and intermediary services as a business, such businesses must obtain registration as moneylending businesses. 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 derivative 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 are gathered via the internet (see Section IV).
**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.

### 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 cryptocurrency exchange operators. 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:

a) transmission of the picture of the identity confirmation documents (attacked with a face photo) and the picture of the customer’s appearance; and

b) transmission of the IC information and the picture of the customer’s appearance.

IV DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES

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 28 February 2019, there are 64 businesses registered as fund transfer service providers in Japan. In early 2019, the government announced its direction to introduce new licence in 2020, under which the maximum amount of fund transfer would not be limited.

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 transfers’ in Japan and thus do not require registration as fund transfer service providers. Many businesses, such as convenience stores, provide these 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.

Acquirers and PSPs

Japan requires credit card issuers to be registered as ‘comprehensive credit purchase intermediaries’. The amendment of the Installment Sales Act 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. 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.
iii  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:

- a monetary contribution (or monetary equivalent) from investors;
- b business using the contributions; and
- c 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 (CRYPTOASSETS) AND INITIAL COIN OFFERINGS

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), may fall under the regulations of the PSA or FIEA depending on how they are structured. Businesses involved in ICOs 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 cryptocurrencies under the PSA, prepaid payment instruments and securities (especially CIS). As mentioned below, these categories will be reorganised and new regulations will be introduced in the near future.

ii Cryptocurrency exchange businesses
Amendments to the PSA to define cryptocurrency and regulate cryptocurrency exchange businesses came into effect on 1 April 2017.

Definition of cryptocurrency under the PSA
The PSA defines cryptocurrency as an electronically recorded proprietary value other than legal currency and assets denominated in any legal currency that either:

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 cryptocurrency); or

b is mutually exchangeable with a type I cryptocurrency between unspecified persons and is transferable through an electronic network (type II cryptocurrency).
Cryptocurrency exchanges
A ‘cryptocurrency exchange business operator’ means one that engages in the business of: (1) selling and purchasing cryptocurrency or exchanging cryptocurrency with another cryptocurrency; (2) acting as intermediary, broker, or agent for the services in item (1); or (3) managing the monies or cryptocurrencies of users in connection with items (1) or (2).

Cryptocurrency exchange operators must manage the funds and cryptocurrencies deposited by users separately from the operators’ own funds and cryptocurrencies. As of 25 March 2019, there are 19 companies registered as cryptocurrency exchange operators in Japan. The FSA did not accept registration of the applicant exchanges and strengthened its role in supervising and inspecting cryptocurrency exchanges in 2018, but has gradually restarted the examination process. In 2018, two major cryptocurrency-related businesses industry groups merged and set up strict self-regulations to restore public and regulatory confidence in cryptocurrency business.

iii Revision of the PSA and FIEA
The environment surrounding cryptocurrency faced several issues in 2018, including multiple cases of theft of customer assets from cryptocurrency exchanges, the realisation that internal control at cryptocurrency exchanges was not keeping pace with the sudden increase in transactions, cryptocurrencies becoming a source of speculative trading owing to wildly fluctuating prices, and the appearance of new types of transactions using cryptocurrency such as ICOs and margin trading. Based on these issues, the FSA released a report examining the future direction of cryptocurrency regulation in Japan, and revisions to the PSA and FIEA based on such report were submitted to the Diet in March 2019.

The bills propose that the legal term ‘cryptocurrencies’ be replaced by ‘cryptoassets’. It also proposes imposing obligations on 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).

Similar to regulations governing the shares of listed companies, the bills also propose introducing regulations against unfair spot 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. They would also prohibit cryptoasset exchanges from engaging in transactions for the purpose of obtaining a profit based on information that has not been made public.

The bills propose widening the scope of cryptoasset management regulations and anti-money laundering regulations to also cover custody services for cryptoassets, requiring them to be registered. It also proposes requiring registration for exchanges engaged in margin trading of cryptoassets and introducing restrictions on such activities, as in the case of foreign exchange margin trading.

Regarding ICOs, the bills propose establishing different regulations for security tokens and exchange tokens. When soliciting 50 or more persons to purchase security tokens, the issuer would be required to file regulatory disclosures at the time of issuance and on
a continuous basis thereafter. Brokers of security tokens would be subject to the same operational restrictions as traditional securities brokers. ICO transactions would be subject to regulations concerning unfair transactions equivalent to those governing traditional securities. Exchange tokens would be required to be exchanged on registered cryptoasset exchanges, in the same way as current regulations. Cryptoasset exchanges would be required to provide proper information such as feasibility of the businesses using such exchange tokens.

The revisions to the PSA and FIEA are scheduled to be deliberated by the Diet as early as 2019, and may be entered into force in 2020 at the earliest.

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 protection in certain cases. 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’.
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 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>November 2017</td>
<td>A financial system study group was established by the FSA, which began studies into changing the legal framework relating to the financial system into one that is functional and cross-sectional (see Section IX below).</td>
</tr>
<tr>
<td>March 2018</td>
<td>Policies are being announced by various banks relating to coordination and collaboration with electronic settlement agents aimed at open APIs (application programming interfaces).</td>
</tr>
<tr>
<td>June 2018</td>
<td>The amended Banking Act came into force, with provisions concerning a registration system for electronic settlement agents and how such system relates to banks. Banks and electronic settlement agents started to enter into agreements for using API provided by banks, required by the amended Banking Act. The amended Installment Sales Act also came into force, with provisions concerning a registration system for acquirers and certain PSPs. The financial system study group of the FSA released a white paper about revision of the legal framework relating to the financial system.</td>
</tr>
<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 will be 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 company.</td>
</tr>
<tr>
<td>March 2019</td>
<td>Bills to amend the PSA and FIEA were proposed in March 2019, in accordance with the white paper released by the cryptocurrency exchanges study group of the FSA.</td>
</tr>
</tbody>
</table>

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. Legislation is scheduled to be proposed in line with these proposals, and the remaining discussion points will continue to be examined by the financial system study group.

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 when opening 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.

iv Cryptocurrencies (cryptoassets) and ICOs

In June 2018, the FSA released a report examining regulations surrounding cryptocurrency transactions. Draft amendments to the FIEA based on such report were submitted to the Diet in March 2019. See Section V for details.
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.

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.

1 Dilmun Leach is a group partner at Collas Crill LLP.
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.
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:

a. that person notifies the Commission in writing that he or she intends to carry on money service business; and

b. 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:

a. the end of the first 18 months after the person begins to carry on the business; or

b. 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:

a. 10 months after the end of that person’s last completed financial period for which the turnover is £300,000 or more; or

b. 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:

a an invitation is made to the public where it is not addressed exclusively to a restricted circle of persons; and

b 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:

a the offer;

b the capital of the issuer;

c any amounts written off or provided for in respect of goodwill or preliminary expenses, or of any benefit given to a promoter;

d material contracts;

e interests of directors;

f debentures and loans of the issuer;

g the company’s latest accounts, including notes on any unusual risks to the investor;

h registered office (and principal operating establishments);

i directors and secretary;

j advisers (including the name and address of the issuer’s auditors, legal advisers and principal bankers);

k date of issue; and

l 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 Electronic Communications (Jersey) Law 2000 (the Communications Law) allows for contractual offer and acceptance to take place by way of an electronic communication (which includes e-signatures).

The Communications Law gives the attributes of an electronic communication as being of its originator if it was dispatched:

a by its originator;
b by a person who had authority to act on behalf of its originator in respect of the communication; or
c by an information system programmed by or on behalf of its originator to operate automatically.

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 e-signature (a 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.
IV CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

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 a right to participate in the profits or earnings of the ICO issuer or a related entity;
b a claim on the issuer or a related party’s assets;
c a general commitment from the ICO issuer to redeem tokens in the future;
d involvement in the ownership or running of the ICO issuer or a related party; and
e 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 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
b a cryptocurrency token, in other words, the token is designed to behave like a currency, referred to in some jurisdictions as a payment token.

i General requirement for all ICO issuers

To ensure consistency and provide a streamlined COBO application process, the Guidance requires all ICO issuers to:

a be incorporated as a Jersey company (i.e., not be a foundation or limited partnership or other form of vehicle);
b receive a consent under COBO before undertaking any activity;
c apply relevant AML or CFT requirements to persons that either purchase tokens from or sell tokens back to the issuer of those tokens;
c appoint and maintain a duly regulated Jersey CSP;
d 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:

- the proposed activity including relevant timelines;
- details of the issuer and the ICO;
- the rationale for the ICO, amount to be raised and use of proceeds;
- a summary of the features of the tokens;
- a summary of purchase and redemption processes;
- service providers to the issuer;
- the relationship between the issuer and the holder of the tokens;
- the management of underlying assets and security rights over such assets for holders of the tokens;
- how the activity will be wound up or dissolved and assets distributed to the holders of the tokens; and
- 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:

- the honesty and integrity of the issuer and the persons associated with it;
- the issuer’s approach to acting in the best interests and needs of each and all of its customers;
- the adequacy of the issuer’s financial and non-financial resources;
- how the issuer will manage and control its business effectively, and ensure that it will conduct its business with due skill, care and diligence;
- the effectiveness of the issuer’s arrangements in place for the protection of client assets and money when it is responsible for them;
- 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

h 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;

k whether the issuer will be an AIF for the purposes of AIFMD; and

l 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 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).

VI YEAR IN REVIEW

The key development in Jersey affecting fintech in 2018 has been the progress made on the regulation of STOs and ICOs. In July 2018, guidance from the JFSC was published on
its approach to the regulation of ICOs, and in October 2018 a new application form was published to allow potential ICO issuers to apply for the relevant consents required under COBO.

This year, Jersey also introduced new legislation to revamp its regime relating to limited liability partnerships (LLPs), which came into force on 1 August 2018. The government is also looking to introduce a new legal entity to Jersey’s repertoire, the limited liability company (LLC).

LLPs have been a feature of Jersey law for some time, but the new law will make the vehicle more attractive to businesses that are considering basing themselves in Jersey. Some of the key changes are:

\[a\] members can now contribute ‘capital, effort and skill’, whereas previously they were required to contribute ‘effort and skill’. This means that business founders can now go into partnership with investors who will provide the necessary capital, without having to get involved in the day-to-day running of the partnership; and

\[b\] under the old Jersey LLP law, LLPs had to make an annual statement confirming that they were solvent and could pay their debts as they fell due. Currently, an LLP only has to make such a statement if a member is planning to make a withdrawal of partnership capital.

LLCs are popular in the United States, and now Jersey is planning to introduce its own version of the vehicle. LLCs are often described as a hybrid between a company and a partnership; unlike a traditional company, the Jersey LLC is governed by an LLC agreement that the members are largely free to agree among themselves.

Under current proposals, the Jersey LLC is likely to share some important features with its US counterparts. Most notably it will have the ability to create series, each with its own separate legal personality, giving businesses the ability to ring fence certain projects if they wish. Perhaps most importantly in the US-centric world of the technology sector, the LLC will provide a vehicle that potential partners or investors based in the United States will know and understand.

VII OUTLOOK AND CONCLUSIONS

The willingness of the JFSC to set out a pathway for Jersey to become an important centre for launching STOs, ICOs and virtual currency exchanges, combined with previous pro-fintech developments (such as the introduction of the regulatory sandbox for digital currency exchanges), has continued Jersey’s development as a pro-fintech jurisdiction.

Jersey’s growing appeal as a technology friendly jurisdiction has been underlined by Binance, the world’s largest cryptocurrency exchanger, establishing itself in Jersey in 2018. This adds to Jersey’s already impressive credentials as a pro-fintech jurisdiction with Global Advisors, a leading crypto fund manager, and SoftBank, the world’s largest technology fund, already based in Jersey.

The introduction of LLPs and LLCs further enhances Jersey’s appeal as a jurisdiction that offers flexibility in the choice of structuring options available to technology businesses, while also offering a regulatory regime that is globally respected. The outlook for Jersey’s technology sector is undoubtedly bright.
I \hspace{1em} \textbf{OVERVIEW}

Currently, there are no prohibitions or restrictions for certain types of fintech businesses in 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 Korea. The Korean government 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 18 key projects for ‘financial innovation’ to be implemented as part of their 2018 business plan, and support for the fintech industry is one of FSC’s key initiatives.

In terms of specific fintech-friendly policies, the Special Act on Support of Innovation of Finance (the Special Act), enacted in December 2018 and enforced from 1 April 2019, introduced the regulatory sandbox scheme in Korea. The new law introduces expedited confirmation on regulation and relaxed regulatory standards for those financial services designated as innovative financial service by the government.

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 businesses in Korea. Notably, small- and medium-sized businesses established in certain areas of 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 Korea. For certain R&D costs (including labour costs and material costs), R&D tax deduction may be available as well.

Despite promoting policies conducive to fintech businesses, however, the Korean government has also shown concern for anti-money laundering and other consumer protection.
matters. The FSC amended the Anti-Money Laundering Guidelines for Cryptocurrencies (AMLC Guidelines) in 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. Also, the peer-to-peer (P2P) Loan Guidelines were amended in 2019 to expand the scope of disclosure for P2P lenders.

Currently, several P2P loan and cryptocurrency related bills are pending at the National Assembly. While it remains unclear when or if these pending bills will be enacted into law, if passed, they may provide a more coherent framework for the regulation of fintech-related issues in Korea.

II REGULATION

i Licensing and marketing

Currently, there are no prohibitions or restrictions for certain types of fintech businesses in 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 Korea. The EFTA covers the:

a rights and obligations of the parties to an electronic financial transaction;
b provisions to ensure the safety of electronic financial transactions and protection of users; and
c authorisation, registration and specific scope of activities of electronic financial businesses.

Activities listed as ‘electronic financial business’ under the EFTA include the:

a issuance and management of electronic currency;
b electronic funds transfer services;
c issuance and management of electronic debit payment services;
d issuance and management of electronic prepayment services;
e electronic payment settlement agency services;
f depository service for settlement of transactions; and
g 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 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 Cross-border issues

Where a fintech business established out of Korea wishes to access new customers in Korea, it will need to consider whether it requires authorisation from a Korean regulatory authority. A fintech business established outside of Korea may be subject to Korean laws and regulations if it carries out regulated activities in Korea. Where an overseas fintech business performs
regulated activities in Korea, it will need to obtain authorisation from the relevant Korean financial regulatory authority, as discussed in Section II(i) above. Generally, the standard 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 Korea and a foreign country. The Foreign Exchange Transaction Rule (the FX Rule) is a subordinate regulation of the Foreign Exchange Transaction Act. The FX Rule was most recently amended in December 2018, and went into force as of 1 January 2019. The current FX Rule increased the annual limit for overseas remittance by institutions registered as small-amount remittance operators from US$20,000 to US$30,000. Also, since 2019, securities companies and credit card companies may remit funds overseas as long as the amount does not exceed US$3,000 per remittance and US$30,000 per year. In addition, electronic currencies and prepaid electronic payment means issued in Korea may now be used in foreign jurisdictions to pay for goods or services or be exchanged to foreign currencies.

III DIGITAL IDENTIFICATION AND ONBOARDING

There is no digital identity that is generally recognised in 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, cell 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, FUNDING AND PAYMENT SERVICES

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 won per year through crowdfunding. To raise funds that exceed 1.5 billion won, conventional means of financing should be utilised. Moreover, under the FSCMA, the issuance of equity for crowdfunding is permitted for non-listed small- to mid-sized companies with less than seven years of business operations.

In 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 won to 10 million 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

There are currently no laws or licences that directly regulate regarding P2P, but there is a plan by the Korean authorities to push forward with P2P loan legislation in 2019. Currently, regulations are based on the Act on Registration of Credit Business and Protection of Finance Users (the Credit Business Act), which applies to general lending businesses, and the P2P Loan Guidelines announced by the FSC in February 2017. Thus, typically, in order to run a lending business, a credit business registration (licence) is necessary in accordance with the Credit Business Act. However, in the case of running a P2P lending business in accordance with the P2P Loan Guidelines, the supervising authority’s position is that it shall not take issue with whether a P2P business or P2P lending investor owns a Credit Business Act licence.

P2P lending that is in accordance with the P2P Lending Guidelines takes place by a method wherein the investor and the borrower do not enter into a direct agreement. Because P2P broker businesses do not have Credit Business Act licences, a liaison financial business operator that has completed registration in accordance with the Credit Business Act enters into a lending agreement with the borrower, and the P2P broker business acts as an intermediary in this arrangement. The investor is not party to the lending agreement with the borrower, but obtains the right to acquire principal and interest that result from the loan bond against the borrower.

The main contents of the P2P Guidelines are as follows:

a investment limits:
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 certain laws (Article 117-10, Item 7 of 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.

iv 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 AND INITIAL COIN OFFERINGS

There is no existing regulatory regime or statute that specifically regulates cryptocurrency or blockchain businesses in 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 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, key developments of which are discussed below.
Cryptocurrencies

In 2017, 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 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 30 January 2018, the Korean Financial Intelligence Unit 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 in June 2018, which took into effect in July 2018 and will remain effective for a year. 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 in case 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.
Currently, there are several cryptocurrency bills proposed at the National Assembly. These bills generally cover, among other things, licensing requirements for cryptocurrency businesses, anti-money laundering requirements, consumer protection, cybersecurity requirements for cryptocurrency exchanges and damage compensation for consumer losses. It is unclear when or if these pending bills, in their current form, will be enacted into law in Korea.

**ii Initial coin offerings**

In September 2017, the FSC issued a press release prohibiting ICOs in 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 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 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 won to 1.5 billion 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 business

The FSC announced its plan to introduce Own Credit Information Management Businesses (known as ‘My Data’) through amendment of the Electronic Financial Transactions Act in order to foster industries for promotion of data payments and to innovate data usage-related regulations.

My Data businesses are businesses that provide professional support for the individual that 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 his or her credit situation, financial status, etc., and compare in detail prices and benefits of each product to recommend financial products optimised for each individual.

In case of providing such financial product comparison services, it is necessary to receive consent from each consumer regarding provision of information on his or her financial situation.

VII. INTELLECTUAL PROPERTY AND DATA PROTECTION

i. Intellectual property

In 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 the Patent Act, fintech inventions relating to software or business methods are generally patentable if they meet the statutory requirements such as subject matter, novelty, and inventiveness. If an invention is not sufficiently creative or inventive to meet the standards of patentability, protection may be available under the Utility Model Act. The basic difference between a utility model and a patent is that a utility model requires a lower technical content. However, fintech inventions that are mainly software or business methods may not be eligible for utility models.

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 any formality. 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 UCPA. The UCPA 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
- whose secrecy is maintained through reasonable effort.

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 Korea against third parties unless it is recorded at the Korean Intellectual Property Office.

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 program works 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 Korea. For copyrights, works by foreigners, such as the source code of fintech software, are entitled to protection under treaties to which 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 force and entitled to protection under the Copyright Act, if the copyright protection period granted in the country of their origin has already expired, 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. As for licence terms, there are no statutory or regulatory restrictions on a maximum royalty rate or payment terms. Further, Korean courts have not issued a ruling on a maximum royalty rate. Thus, the parties may agree on royalty rates and payment terms based on the facts in individual cases.

**ii Personal data**

In 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 Korea that may apply to fintech businesses operating in 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, there are various sector-specific privacy laws such as the Act on the Promotion of IT Network Use and Information Protection (the Network Act) and the Use and Protection of Credit Information Act (the Credit Information Act) that complements the PIPA. The Network Act regulates the processing of personal information in the context of services provided by online service providers (e.g., personal information collected through a website). The Credit Information Act regulates and protects financial transaction information and credit information of individuals and entities. Both the Network Act and the Credit Information Act can apply to fintech businesses operating in Korea.

The Ministry of the Interior and Safety is responsible for enforcing the PIPA. The Korean Communications Commission and the Ministry of Science and ICT are responsible for enforcing the Network Act. The FSC and the FSS are responsible for enforcing the Credit Information Act. Each of these regulatory agencies can make requests for information and conduct inspections at the premises of data controllers to ensure they are compliant with the respective privacy laws. In addition, once a violation of a relevant privacy law is confirmed, each of these respective regulatory agencies 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. In addition, sector-specific privacy laws such as the Network Act would apply to overseas online service providers collecting personal information in Korea. Further, the Credit Information Act would also apply to overseas entities handling financial transaction information and credit information of individuals or entities in Korea. Although the PIPA, the Credit Information Act, and the Network Act do not specifically address their jurisdictional scope for overseas entities, the Korean regulatory authorities have measures to ensure compliance by overseas entities with these laws.

### Cybersecurity

The main statutes in the context of cybersecurity that apply to fintech businesses are the PIPA and the Network Act. The PIPA and the Network Act prescribe detailed technical security and administrative requirements for cyber security 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 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.

### VIII YEAR IN REVIEW

Over the past 18 months, notable amendments were made to financial laws that may impact fintech businesses operating in Korea. Specifically, in April 2018, the Enforcement Decree of the FSCMA was amended to increase the limit for ordinary investor’s investment in crowdfunding by 100,000 won. As a result, an ordinary investor may now invest 5 million won per year for an issuer of equity. Also, the Foreign Exchange Transaction Rule (the FX Rule), a subordinate regulation of the Foreign Exchange Transaction Act, was most recently amended in December 2018 and took into force as of 1 January 2019. The current FX Rule increased the annual limit for overseas remittance by institutions registered as small-amount remittance operators from US$20,000 to US$30,000. Further, since 2019, securities companies and credit card companies may remit funds overseas as long as the amount
does not exceed US$3,000 per remittance and US$30,000 per year. In addition, electronic currencies and prepaid electronic payment means issued in Korea may now be used in foreign jurisdictions to pay for goods or services or be exchanged to foreign currencies.

Along with changes to financial laws, amendments were also made to guidelines concerning cryptocurrency and P2P loans. The FSC amended the AMLC Guidelines in June 2018, which took into effect in July 2018 and will remain effective for a year. Among other requirements, the AMLC Guidelines mandated enhanced monitoring by financial institutions for accounts of cryptocurrency companies used for operating expenses and sharing of the list of foreign cryptocurrency companies among financial institutions. The P2P Loan Guidelines were also amended in 2019 to expand the scope of disclosure for P2P lenders. In particular, the 2019 P2P Loan Guidelines recommend that P2P lenders disclose outside expert’s review of key features of PF loans and disclose real estate P2P loan products for two days prior to sale. In addition, the 2019 P2P Loan Guidelines recommends P2P lenders to hire third-party experts to audit the P2P lender’s protection of online personal information at least once a year and disclose the result of the audit.

Furthermore, there are currently several cryptocurrency and P2P loan-related bills proposed at the National Assembly. Specifically, the FSC announced in 2019 that they will recommend a comprehensive bill regulating P2P loans to the National Assembly based on the five current bills related to P2P loans that are pending at the National Assembly. Cryptocurrency bills have also been proposed at the National Assembly, generally covering, among others, licensing requirements for cryptocurrency businesses, anti-money laundering requirements, consumer protection, cybersecurity requirements for cryptocurrency exchanges and damage compensation for consumer losses. However, it is unclear when or if these pending bills, in their current form, will be enacted into law in Korea.

As for its position on ICOs, on 31 January 2019, the Korean government announced the result of its monitoring of the ICO practice in 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 ICO poses high investment risks and lacks 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.

Meanwhile, measures have been taken to promote fintech innovations in the financial services market in Korea. Notably, the Special Act, enacted in December 2018 and enforced from 1 April 2019, introduced the regulatory sandbox scheme in Korea. The new law introduces the following two policies.

i Expedition 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 as an innovative financial service by the government may operate free of regulation or without legal grounds for operation during the designated period (less than two years and may be renewed once for less than two years). Financial service providers who believe that their service is clearly distinguished from pre-existing service in terms of contents and methods may ask the government to designate such service as an innovative financial service. Upon receiving an application, the Innovative Financial Services Examination Committee, which consists of public of 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 Korea;
- whether the proposed financial services is truly innovative; and
- whether the proposed financial service will likely increase the customers’ interests.

In addition, if a designated innovative financial service is being operated under a licence required by other financial laws and regulations, such designated innovative financial service shall be afforded 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.

IX OUTLOOK AND CONCLUSIONS

Recently in Korea’s fintech environment, a variety of industries have been established, and the related market is developing explosively. Korea’s financial supervisory authorities have recently announced various policies to promote fintech. Also, the Special Act, which institutionalises the ‘sandbox policy’ to promote development and advancement of innovative financial services was enforced from 1 April 2019. Under the Special Act, the ‘expedited confirmation on regulation policy’ is introduced, wherein 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 Special Act also introduces the ‘designation of innovative financial service policy’, wherein a financial service that is designated as an innovative financial service by the government may operate free of regulation or without legal grounds for operation during the designated period (less than two years and may be renewed once for less than two years).

Furthermore, there are currently two internet-only banks in Korea, K-Bank and Kakao Bank, that have received authorisation and are in operation. Around late March, the FSC plans to solicit pre-authorisation applications for new internet-only banks and authorise up to two internet-only banks.

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 hesitance 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.
A number of proposed pieces of legislation covering cryptocurrencies are pending at the National Assembly. These bills generally cover licensing requirements, anti-money laundering requirements, consumer protection, cybersecurity requirements and compensation for consumer losses. For example, a bill entitled the Special Act on Cryptocurrency Business seeks to, *inter alia*:

- impose a requirement that a licence be obtained for cryptocurrency exchanges and cryptocurrency-related businesses;
- impose record-keeping obligations;
- explicitly incorporate cryptocurrency businesses into the AML Act and other laws regulating financial institutions; and
- mandate the adoption of cybersecurity measures, among other things.

If passed, these bills may provide a more coherent framework for the regulation of cryptocurrencies and other related issues.
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 18 per cent on the basis of their worldwide income (owing to a decrease of 17 per cent in 2019). However, companies that earn profits not exceeding €25,000 (expected to increase to €175,000 in 2019) 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 should be added, making the aggregate corporate tax rate amount 26.01 per cent (expected to decrease to 24.94 per cent in 2019). 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, Konstantinos Georgiou is an 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:

- the Luxembourg Law of 10 November 2009 on payment services, as amended (the 2009 Law);
- the Luxembourg Law of 5 April 1993 on the financial sector, as amended (the 1993 Law);
- CSSF-related regulations and circulars, provided that their activities fall within the scope of the above-mentioned laws;
- the Luxembourg Law of 7 December 2015 on the insurance sector (the 2015 Law);
- the Luxembourg Consumer Code (the Consumer Code); and

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 (the 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:

- the applicant fulfils the legal conditions for qualification (when required) and professional integrity for the activity concerned; and
- 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:

- 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.

**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).

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).3

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.

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:

---

3 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.


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.4

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).5

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.6

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.7

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.

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

---

4 Article 30(2) of the 1993 Law.
5 Article 31 of the 1993 Law.
6 Article 32(1) of the 1993 Law.
7 Article 32(5) of the 1993 Law.
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:

a. it is permitted within its jurisdiction to provide investment services and engage in investment activities that it wishes to offer to Luxembourg;

b. it is subject to supervision and authorisation requirements that the CSSF considers equivalent to those of the 1993 Law; and

c. 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.

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

---

8 Article 32(1) of the 1993 Law.
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).10

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:

\[a\] they perform the video identification process themselves using a tool developed internally;

\[b\] they perform the video identification process themselves using an external tool acquired from an external provider; or

\[c\] they delegate the identification process to an external provider using their own tool.

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, FUNDING AND PAYMENT SERVICES**

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.

11 CSSF FAQ on Securitisation, What are the various possible forms of debt securitisation?, p.7.
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.\(^\text{13}\)

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 AND INITIAL COIN OFFERINGS

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 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

\(^{12}\) AIFM Law means the Luxembourg law of 12 July 2013 on alternative investment fund managers.

\(^{13}\) CSSF FAQ on Securitisation, 19. What is the impact of the law of 12 July 2013 on alternative investment fund managers (the AIFM Law) on the securitisation undertakings within the meaning of the 2004 Law?, p.14.

\(^{14}\) Loi du 1er mars 2019 portant modification de la loi modifiée du 1er août 2001 concernant la circulation. de titres.
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 proceed 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: a the consent of the party who binds himself or herself; b his or her ability to sign the contract; c a specific purpose or object for contracting; and d 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:

a) imposes the free determination of the price of goods, products and services based on free competition;

b) 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

c) 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.

i PSD II

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.

ii Anti-Money Laundering Directive IV

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.


iii  Circulation of securities
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.

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 involve (whether based on European positions or not) around tokenisation and the structures issuing or using tokens.
I OVERVIEW

The Malaysian government has long understood the importance of building up its financial sector. It is fair to say that the respective regulators of the financial and capital markets sectors have encouraged fintech developments and, where necessary, proactively adjusted the regulatory framework to facilitate its growth. For example, the Malaysian Securities Commission (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 (BNM) and the SC are the main regulatory bodies that regulate licensing and marketing requirements for fintech companies. Their recent regulatory decisions demonstrate a measured approach to regulating innovations in these industries.

There are two main developments in the regulatory aspect of fintech businesses in Malaysia. First, the BNM, through the Financial Technology Enabler Group, launched a financial technology regulatory sandbox (the Regulatory Sandbox) in 2016, seeking to provide a regulatory environment that is conducive for the deployment of fintech as the end goal. As part of this process, the Regulatory Sandbox Framework (the Framework) was introduced to enable the innovation of fintech to be deployed and tested in a live environment, within specified parameters and time frames. The Framework is applicable to financial institutions and fintech companies approved for participation by the BNM. Successful applicants will be given an approval to test solutions in a live market within a period not exceeding 12 months.

Second, pursuant to the Capital Markets and Services Act 2007 (CMSA 2007), the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 (the Order 2019) was gazetted and came into force on 15 January 2019. Pursuant to Order 2019, digital currencies and digital tokens that are not issued or guaranteed by any government body or BNM, and fulfils other specific features, are prescribed as securities. The implications of treating digital currencies and digital tokens as securities are significant, as the CMSA 2007 would apply. Thus, digital currencies and digital tokens will be regulated by the SC, affecting how they can be offered and traded in Malaysia moving forward.

---

Shanthi Kandiah is a partner at SK Chambers. She was assisted in writing this chapter by Henin Tong, Denishia Rajendran and Nimraat Kaur.
There are no known tax incentives specifically catered to fintech companies. However, there are tax incentives and preferential tax rates available for small and medium enterprises (SMEs), which could be applicable to fintech start-ups depending on their business areas. Relevant fiscal incentives are as follows:

- The angel tax incentive granted to angel investors in technology-based start-ups administered by Cradle Fund Sdn Bhd. It is designed to encourage more investments from the private sector into early stage companies in technology space; and
- The Malaysia Digital Economy Corporation Sdn Bhd (MDEC) offers corporate tax exemption for technology start-ups in the Malaysian Digital Hub.

There are also the Multimedia Super Corridor (MSC) Malaysia tax incentives offered for MSC Malaysia status companies in information and communications technology (ICT) and ICT-facilitated businesses. Following from Malaysia’s participation in the Organisation for Economic Co-operation and Development Base Erosion and Profit Shifting taxation initiatives, the new legislation and guidelines for MSC Malaysia tax incentives are currently being reviewed by the government and further information will be released in due course.

As an initiative to promote Malaysia as a hub for technology start-ups, MDEC has introduced the Malaysia Tech Entrepreneur Programme to attract entrepreneurs worldwide in the technology industry to establish their start-ups and expand their business within the ASEAN region.

II REGULATION

i Licensing and marketing

A large number of fintech players in Malaysia are involved in payments and cryptocurrency sectors. A fintech company should always consider in advance whether a licence from a regulatory authority is required as there is no one-size-fits-all licence that applies to every fintech player. The issues with licensing will depend on the specific scope of activities of the fintech product or service the company has to offer. Generally, 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 can be issued in different forms such as a digital wallet (e-wallet), which is a type of pre-paid account in which a user can store their money for any future online transaction.</td>
<td>BNM</td>
<td>E-money issuers must obtain approval from BNM pursuant to Section 11 of the Financial Services Act 2013 (FSA 2013). According to Division 1, Part 1, Schedule 1 of the FSA 2013, businesses that require approval includes issuance of a designated payment instrument.</td>
</tr>
<tr>
<td>Merchant acquiring service – a third party that facilitates merchants in accepting payments.</td>
<td>BNM</td>
<td>Merchant acquiring services is one of the registered business under Schedule 1, Part 2 of 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>SC</td>
<td>Under the Guidelines on Recognised Markets (the Guidelines), released pursuant to CMSA 2007, ECF operators must register as a recognised market operator (RMO) with the SC.</td>
</tr>
<tr>
<td>Fintech service</td>
<td>Regulatory body</td>
<td>Licensing/approval/registration</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Property crowdfunding – 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>SC</td>
<td>The SC released a Public Consultation Paper on 6 March 2019, the ‘Proposed Regulatory Framework for Property Crowdfunding’ (Consultation Paper on Property Crowdfunding). The SC is seeking feedback on the proposed regulatory framework for property crowdfunding activities.</td>
</tr>
<tr>
<td>Digital assets* offered through initial coin offerings (ICOs) – an issuer, typically an early-stage venture, creates and issues its own digital assets in exchange for established digital currency (e.g., bitcoin or ether) or fiat currency.</td>
<td>SC</td>
<td>The SC released a Public Consultation Paper on 6 March 2019, the ‘Proposed Regulatory Framework for the Issuance of Digital Assets Through Initial Coin Offerings (ICOs)’ (Consultation Paper on ICOs). It seeks to provide background as to the nature of digital assets, the risks involved in investing in digital assets and the proposed regulatory framework on ICOs.</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>SC</td>
<td>Under the Guidelines, a P2P operator must register as a RMO with the SC.</td>
</tr>
<tr>
<td>Digital Asset Exchange (DAX) – online platforms where digital currencies and digital tokens are traded.</td>
<td>SC</td>
<td>The SC regulates DAX platform operators. Under the Guidelines, digital exchanges must be registered as an RMO with the SC.</td>
</tr>
<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>SC</td>
<td>DIM is a regulated activity pursuant to Part 1, Schedule 2 of CMSA 2007, and as such must obtain a capital markets services licence from the SC pursuant to Section 58 of CMSA 2007.</td>
</tr>
</tbody>
</table>

* According to Chapter 15: Digital Asset Exchange of the Guidelines, digital asset refers collectively to a digital currency or digital token, which are both defined in the Order 2019.

Credit information services

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 furnishes 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).

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 (the CRAA 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.

---

2 Section 47 of the CBA 2009.
Cloud computing

Cloud computing delivers computing services, such as managing and storing data and access to applications, over the internet via the cloud. Cloud computing for financial services companies is permitted in Malaysia. The BNM regulates cloud services, in the context of outsourcing arrangements\(^3\) entered into between companies and cloud service providers. The BNM issued the Policy Document on Outsourcing (the Outsourcing Policy), which came into effect on 1 January 2019 and applies to financial institutions. In the Outsourcing Policy, the BNM has expressed that a key concern to regulators is the over-reliance on service providers for activities that are critical to the ongoing operations and safety of financial institutions.\(^4\) Approval is required from the BNM where fintech companies enter into a material outsourcing arrangement or make a significant modification to an existing material outsourcing arrangement.

A material outsourcing arrangement is defined under the Outsourcing Policy as an outsourcing arrangement that:

\(\begin{align*}
\text{a} & \quad \text{in the event of a service failure or security breach, has the potential to significantly impact the financial institution's provision of financial services to customers, business operations, financial position, reputation or compliance with applicable laws and regulatory requirements; or} \\
\text{b} & \quad \text{involves customer information and, in the event of unauthorised access, disclosure or modification, or loss or theft of the information, has a material impact on the customer or financial institution.}
\end{align*}\)

In conjunction with the Personal Data Protection Act 2010 (the PDPA 2010), the Personal Data Protection Regulations 2013 (the Regulations), which came into operation on 15 November 2013, require that data users develop and implement a security policy for their companies. This security policy must comply with the standards established by the Commissioner of the Department of Personal Data Protection (the Commissioner) from time to time.\(^5\) Some of the more prescriptive standards for implementation stipulate that transfer of personal data through cloud computing services is no longer permitted, unless authorised in writing by the top management of the company.

Digital advisory or asset management company

DIM is a form of fund management that is a regulated activity 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.

In 2018, StashAway Malaysia was the first DIM company to obtain a capital market services licence from the SC to commence operations.

Crowdfunding P2P

Pursuant to the Guidelines, ECF operators and P2P operators must be registered as a RMO as they provide an alternative trading venue or marketplace that brings together purchasers

---

\(^3\) Paragraph 5.1 of the Outsourcing Policy defines ‘outsourcing agreement’ as an arrangement in which a service provider performs an activity on behalf of a financial institution on a continuing basis.

\(^4\) Paragraph 1.3 of the Outsourcing Policy.

\(^5\) The Personal Data Protection Standards 2015.
and sellers of capital markets products. The Guidelines set out the registration requirements for ECF and P2P operators and funding limitations for investors. Currently, there are seven ECF platforms and six P2P platforms registered with SC as a RMO.

An issuer hosted on a P2P platform will issue an investment note to investors as evidence of a monetary loan executed on the platform. Investment notes are prescribed as securities by virtue of the Capital Markets and Services (Prescription of Securities and Islamic Securities) (Investment Note and Islamic Investment Note) Order 2016, which came into force on 16 May 2016.

In the Consultation Paper on Property Crowdfunding, the SC proposes that property crowdfunding operators must be registered as RMOs pursuant to the Guidelines. The SC also proposes several regulatory requirements to be imposed in relation to platform operators (e.g., criteria to qualify, obligations, permissible activities), homebuyers (e.g., criteria, funding limit, obligations) and criteria on the type of properties that can be hosted on the platform. FundMyHome is an example of a property crowdfunding platform based on P2P principles. It enables a first-time home buyer to acquire a property for 20 per cent of the property price. The remaining 80 per cent will be fulfilled by interested investors in exchange for the potential appreciation in the property’s value over a period of five years. When the five-year period expires, the property owner can choose to sell the property or stay by refinancing the property.

**Insurtech**

Insurtech refers to the use of technology innovations designed to squeeze out savings and efficiency from the current insurance industry model. Digital distribution of insurance products benefits the society by making information more accessible, lowering price barriers, unbundling insurance products and shaping healthier behaviours in the long run. Some of the established insurers such as Etiqa Insurance Bhd, Maybank Ageas Holdings and Zurich Malaysia have partnered up with fintech start-ups to provide platforms enabling users to customise insurance policies and to obtain the best insurance products in proportion to the income earned by the user. There are also start-ups such as Ringgitplus and GoBear that provide platforms for consumers to compare and contrast the available insurance policies in the market in a more layman friendly manner, according to factors such as coverage terms and payment plans.

However, insurtech is not limited to consumers purchasing insurance products directly from an insurer. It extends to the business-to-business ecosystem where insurers are working with those beyond the insurance industry to offer new solutions. For example, Allianz Malaysia partnered with local start-ups Recommend.my, an online service provider platform. Those who book services from Recommend.my will automatically receive insurance protection for each transaction.

---

6 According to Chapter 14: Peer-to-peer financing (P2P) platform of the Guidelines, an issuer means a person that is seeking funding on or through a P2P platform and shall include seeking funding via invoice financing.

Marketing of fintech products and services
Marketing of fintech products and services would depend on whether the fintech company is providing services and products that are regulated in Malaysia. Therefore, fintech companies must first recognise whether it provides regulated fintech services and products before they can be marketed.

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. However, the BNM’s Regulatory Sandbox is open to all fintech companies both domestically and internationally.

In March 2017, Malaysia launched the world’s first Digital Free Trade Zone (DFTZ) to help local SMEs get into cross-border trade by leveraging on digital technology and opportunities in e-commerce, and to attract e-commerce transhipment investment into Malaysia. It does so by providing physical and virtual zones to facilitate SMEs to capitalise on the convergence of exponential growth of the internet economy and cross-border e-commerce activities. The DFTZ is a product of collaboration between the MDEC and the Alibaba Group.

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’ permit, replacement of national identity card, payment of parking summons, auto insurance and road tax renewal and temporary transfer 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 October 2018, the Minister for the Communications and Multimedia Ministry (the Ministry), Mr Gobind Singh Deo, announced the Ministry’s plans to formulate a separate national digital identity.

The Minister mentioned that the proposed national digital identity aims to provide a ‘verifiable platform of trust’ to reduce the possibility of fraud which is common in e-commerce transactions. However, the national digital identity provides a platform to verify the identity of an individual, thus reducing the scope of such crimes. The Minister also announced that the national digital identity project will be an integral platform for the digital government initiative, which includes delivering targeted subsidies efficiently via an e-wallet account registered using the national digital identity. The Ministry will cooperate with the
Malaysia

Malaysian Communications and Multimedia Commission and MDEC in the formulation of the national digital identity project. The Ministry intends to finalise the proposal for the national digital identity by mid-2019.

As the project is still being formulated, it is not known whether the digital identity will extend to fintech businesses and non-residents of Malaysia.

Digitised onboarding is a relatively new process in the financial services sector. In 2017, CIMB Bank Berhad (CIMB) was the first Malaysian bank to receive the BNM’s Regulatory Sandbox approval to implement the electronic know-your-customer (e-KYC) method for customer-identity verification. In implementing e-KYC, financial service providers may be subject to 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 CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

The extent to which blockchain technology is regulated is based on the laws applicable to the type of products or services provided. In 2017, the Department of Standards Malaysia – an agency under the purview of the Ministry of International Trade and Industry – has formed a national technical committee on blockchain and distributed ledger technology (DLT), focusing on the development of blockchain standards for the nation.

As mentioned above, digital currencies or digital tokens are only prescribed to be securities if they meet the characteristics set out in Section 3 and Section 4 respectively of Order 2019. In Section 3 of Order 2019, digital currencies are prescribed as securities where:

- they are traded in a place or on a facility where offers to sell, purchase or exchange the digital currency are regularly made or accepted;
- a person expects a return in any form from the trading, conversion or redemption of the digital currency or the appreciation in value of the digital currency; and
- they are not issued or guaranteed by any government body or central banks as may be specified by the Commission.

In Section 4 of Order 2019, a digital token that represents 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 is prescribed as securities 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 banks as may be specified by the Commission.
To further safeguard the integrity of the capital market and protect investors’ interest, the SC proposed a two-pronged approach for ICOs in the Consultation Paper on ICOs. The proposed regulatory framework involves:

- obtaining authorisation from the SC for the offering or issuance of the ICO; and
- the registration of a disclosure document (Whitepaper) prescribing minimum requirements set by the SC.

An ICO issuer has to approach a third party to ‘host’ the ICO and assess its Whitepaper. In this regard, the ICO issuer is required to undergo an assessment conducted by an independent third party authorised by the SC, prior to it submitting a formal application to the SC.

In the event that this proposed regulatory framework is implemented, SC would then be imposing a full control *ex ante* approach over issuances of all kinds of tokens. All types of token-issuance should be registered and authorised by the SC. The opaqueness in characterising the type of digital tokens in the Order 2019 and Consultation Paper on ICOs suggests that the SC is taking a broad approach in including all types of digital tokens as securities.

On 31 January 2019, the Guidelines were amended to include the requirements for DAX operators to be registered as RMOs. Companies that have submitted their application to be registered with the SC as DAX operators will be permitted to continue operations during the transitional period from 1 March 2019 until such period as may be notified by the SC.

The Sector 6 Policy Document, which came into effect on 27 February 2018, was issued pursuant to the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA 2001), FSA 2013 and the Islamic Financial Services Act 2013. Pursuant to the Sector 6 Policy Document, any person offering services to exchange digital currencies is subject to obligations under the AMLA 2001 as a reporting institution. 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.

It remains to be determined if cryptocurrencies are subject to tax laws 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 leeway in the area of cryptocurrency. In an update release dated 12 January 2018 by Luno, a London based digital exchange, 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 IRB had agreed to unfreeze the bank account while in the process of completing the investigation.

V 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.

---

8 https://luno.statuspage.io/incidents/lzzrvb1mq51y.
9 ibid.
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 (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 (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.

There is no regulator for third-party websites comparing or providing information about financial products. However, the activities of price comparator sites are subject to the Competition Act 2010 (CA 2010). The main prohibitions against anticompetitive agreements or abuse of dominance would govern the activities of price comparator 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:

a. price comparator sites have been found to facilitate information exchange between competitors; or

b. the use of most favoured nation clauses leads to one comparator 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.

Such cases will be subjected to intellectual property and personal data protection considerations, which are further discussed in Section VI.

Artificial Intelligence (AI) has made a 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.

VI 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 the 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. There is no system of registration for confidential information as well – business models and software can be protected if they are confidential in nature, disclosed in circumstances importing confidentiality and there is an actual or anticipated unauthorised use or disclosure of the information.

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.

10 Section 7 of the ECA 2006.
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, which is enforced by the Commissioner, is based on a set of data protection principles similar to the European Union principles\(^\text{11}\) and is often described as European-style privacy law. The PDPA 2010 would apply to fintech companies as it provides for the protection of personal data (i.e., client data) in relation to all commercial transactions. A failure to comply with the PDPA 2010 would lead to possible fines or imprisonment.

Apart from the seven principles set out in the PDPA 2010, there are no rules that apply specifically to digital profiling of clients. A data subject\(^\text{12}\) must consent to the processing of the personal data unless the processing is necessary for specific exempted purposes.\(^\text{13}\) Although the PDPA 2010 does not define nor prescribe any formalities in terms of consent, the Regulations provide that the data user must keep a record of consents from data subjects and that the Commissioner or an inspection officer may require production of the record of consents.

Also, 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.

**VII YEAR IN REVIEW**

The following highlights SC and BNM initiatives in the regulation of fintech services in Malaysia.

In December 2018, SC announced the completion of Project Castor formed under SC’s innovation laboratory, Alliance of Fintech Community. Project Castor seeks to explore the feasibility in implementing DLT as the underlying market infrastructure for unlisted and over-the-counter (OTC) markets as decentralised markets. As unlisted and OTC markets are less transparent and liquid when compared with listed markets, the implementation of DLT aims to reduce these challenges. In January 2019, the BNM released its Policy Document on ‘Publishing Open Data using Open API’ (the Policy Document), which set out the BNM’s guidance on the development and publication of Open Application Programming Interface (Open API) for open data by financial institutions. The BNM aims to encourage open banking through the use of Open API, which enables third-party developers to access data without needing to establish a business relationship with financial institutions. The Policy Document provides that the publication of Open Data has the objective to facilitate the development of fintech in allowing consumers to compare a wide range of products and services.

---

\(^\text{11}\) EU Data Protection Directive 95/46/EC.
\(^\text{12}\) Section 4 of the PDPA 2010 defines ‘data subject’ as an individual who is the subject of the personal data.
\(^\text{13}\) Section 6(2) of the PDPA 2010.
services matching their specific needs and circumstances. While not mandatory, financial institutions are encouraged to adopt Open Data API Specifications recommended by the Open API Implementation Groups for credit card, SME loans and motor insurance products.

In March 2018, SC and BNM joined forces to establish the Brokerage Industry Digitisation Group (BRIDGe), which aims to accelerate digitisation in the stockbroking industry in order to enhance operational efficiencies and service standards. According to the former SC Chairman, Tan Sri Ranjit Ajit Singh, the intention of BRIDGe is to create more efficiency in the entire value chain of the brokerage industry, including the way in which investors interact with trading and brokerage businesses.

VIII OUTLOOK AND CONCLUSIONS

The advent of fintech has brought about the need for regulation in the fintech industry. The approach taken by BNM and SC suggests that fintech is being welcomed, albeit in a cautious manner. BNM’s Regulatory Sandbox, for example, clearly demonstrates BNM’s approach in encouraging fintech while carefully monitoring the progress and development of fintech services and products. The Order 2019 and the consultation papers by the SC also aim to create certainty by regulating digital assets and fintech activities under the CMSA 2007. These initiatives will pave the way for a more digitally safe and literate country.

With ECF and P2P platforms coming into play, as well as the gaining popularity of DIM services, Malaysians now have the opportunity to diversify their investment portfolios. The guidelines and regulations of these platforms by SC minimise investment risks and create a more reliable environment for Malaysians to invest their money.
Chapter 17

MEXICO

Federico de Noriega Olea and Juan Enrique Lizardi Becerra

I OVERVIEW

Over the past year, the Law to Regulate Financial Technology Companies (the Fintech Law), and certain secondary regulations were enacted. However, certain secondary regulations are still pending, and are currently under discussion by the administrative bodies in charge of their issuance.

Regulated fintech entities, which are construed as part of the financial services sector, are regulated by four main 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


While it is true that the spirit of the Fintech Law is to permit fintech companies to do business in Mexico, it is also true that Mexican financial authorities’ opinions are still divided on this topic. In our opinion, depending largely on how the laws and 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

1 Federico de Noriega Olea is a partner and Juan Enrique Lizardi Becerra is an associate at Hogan Lovells.
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 will comprise 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 or the risk that they will assume. This permits differentiated regulatory requirements for companies at a different scale or level.

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;
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 they operate through a licensed broker-dealer and they are not custodian of the assets.

Considering the provisions set forth within the Fintech Law, sharing of information will be subject to secondary rules issued by the Supervising Commission and Banxico. Such secondary rules shall be issued no later than March 2020. 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:

- 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;
- 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. Within the Digital National Strategy,2 which is defined as the action plan of the Mexican government to implement a digital nation on which technology and innovation converge to reach the goals for the development of the country, the implementation of a digital identity in the near future is expected to begin but there is no specific deadline. Under the Digital National Strategy, it is envisaged that Mexican citizens may access 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. We expect that fintech companies that provide more

identification methods will be allowed to increase the limits of funds or withdrawals when using the relevant platform. As mentioned before, identification methods may vary but the most common means used by fintech companies are currently:

- online validation of a mobile number;
- ID validation (by taking a picture of the relevant user in conjunction with his or her ID);
- valid proof of address;
- linking a fintech account to a bank account in order to receive or transfer funds; and
- 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.

IV DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES

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:

- 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;
- provide information to the potential investors so that they know the characteristics of the requests of crowdfunding or projects;
- enable and allow electronic means of communications between investors and borrowers;
- obtain loans and credits;
- issue securities;
- own or lease real property;
- make deposits in authorised financial companies;
- create a trust required to comply with their legal purpose (e.g., to segregate funds);
- make investments in complementary, auxiliary or real estate companies;
- perform judicial or extrajudicial collection of credits granted to borrowers by investors, as to renegotiate the terms and conditions of relevant credits; and
- 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;
(g) obtain loans and credits of any local or foreign person in order to comply with their corporate purpose;
(h) issue securities on their own account;
(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 will be subject to secondary regulations that shall be drafted and issued, in the future, 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.

In addition, the Fintech Law provides that CNBV will be the authority in charge of issuing general provisions related to information security, which shall 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 AND INITIAL COIN OFFERINGS

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. This part of the Fintech Law has been subject to debate and there have been some attempts to remove cryptocurrencies and to leave this for further study. We expect Banxico to take longer to issue secondary regulations regarding cryptocurrencies.

The Fintech Law does not define whether cryptocurrencies or other tokens may be considered as securities and does not regulate initial coin offerings. However, we expect this to be regulated in Banxico’s secondary regulation.
Credit institutions approved by Banxico may engage in transactions with cryptocurrencies approved by the latter and in accordance with the general provisions issued by the mentioned Central Bank.

No specific technology is regulated by the Fintech Law. 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:

- it has an innovative model;
- the product or service to be offered to the public shall be tested in a controlled environment;
- the new model represents a benefit to the client that cannot be obtained from existing models available in the market;
- operations may be made immediately;
- the project shall be tested with a limited number of clients; and
- other requirements that are to be determined by financial authorities.

Temporary authorisation shall not be for longer than two years and shall be in accordance with the services that will be or are planned to be provided.

CONDUSEF will be the authority empowered to resolve controversies between authorised authorities to operate an innovative model. Financial authorities may authorise fintech companies, financial entities or others to implement and operate innovative models.

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:

a. has policies and procedures similar to those contemplated by the Data Protection Law and the Data Protection Regulations;

b. 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;  
d maintains confidentiality; and  
e 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

Some of the secondary regulations established under the Fintech Law are still pending, therefore fintech companies will not be able to operate with full legal certainty until all secondary regulations are issued and they are aware of their obligations and the process to obtain and maintain their licences.

In December 2018, there was a change in government in Mexico and a new ruling party came to power. The new government has expressed interest in financial inclusion and financial innovation but there have not been specific pronouncements or guidelines with respect to the Fintech Law and its applications.

To this date, the list of financial services providers does not contain any registered crowdfunding companies or e-money companies, which most likely is a consequence of the regulatory uncertainty that exists until the CNBV and Banxico issue all regulations related to the Fintech Law.

During the course of this year, the CNBV shall issue secondary provisions in connection with:

a the sharing of information to crowdfunding investors; and  
b sharing of information through digital means.

IX OUTLOOK AND CONCLUSIONS

As the Fintech Law is a principle-based law, we anticipate most issues will be 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 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, we are not certain about the criteria that authorities will follow regarding their acceptance. It is not clear
whether methods 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 2019 will be a year of change and progress in this field, and given the quick adoption of fintech and the interest the public has shown in it, we foresee that Mexican users and service providers are likely to increase rapidly.
Chapter 18

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 startups 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.
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,2 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.3 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.4

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.5 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, 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. 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. 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.

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

© 2019 Law Business Research Ltd
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 electronic 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, FUNDING AND PAYMENT SERVICES

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:

a managing a Dutch alternative investment fund (AIF);
b marketing units in an AIF in the Netherlands; or
c 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 only obtain a dispensation from the AFM to conduct such

activities.\textsuperscript{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.\textsuperscript{12}

\section*{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.\textsuperscript{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.\textsuperscript{14}

\section*{V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS}

\subsection*{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.

\subsection*{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.\textsuperscript{15}

A security is defined in Section 1:1 of the AFS, \textit{inter alia}, as a transferable share, or other

\textsuperscript{11} M Williams, Peer-to-peer lending in the Netherlands, \textit{Journal of European Consumer and Market Law}, p. 188.


\textsuperscript{13} Stb. 2019, 60, as amended by Stb. 2019, 114.

\textsuperscript{14} Accidently, 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 must 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.\(^\text{16}\) 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, ‘Vergelijkingsites 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 data23 and is protected under these laws. Data relating to legal entities and deceased24 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 basis25 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.\(^{27}\)

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 startups, 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).
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, containing 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 the Payment Initiation Service Providers (PISP) and the 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 up until now, 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, 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, in partnership with Portugal Fintech (a Portuguese association supporting the emerging fintech ecosystem) with the purpose of establishing an easily accessible communication channel between entrepreneurs and emerging companies and the 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, we have also noticed an increased interest by the regulators in these matters, having been actively engaged in participating in fintech-related conferences and disclosing information coming out of such conferences in their respective websites.

II REGULATION PSEMLF

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 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 range 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 another similar guarantee 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 offered 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), 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 incorporated in Portugal, through authorised agents based in Portugal or under a free provision of services’ licence.

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, more demanding procedure).

In relation to crowdfunding platforms, no cross-border regime is yet foreseen under Portuguese law; this lack of passporting regime requires foreign crowdfunding platforms to have their local registration with the CMVM on standby, until such regime is legally provided for. 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 with 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).

IV DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES

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. 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.

V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

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.

However, the approach in Portugal in this sector has been to 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.

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 done by non-regulated and non-supervised entities. In addition, the Bank of Portugal clarified and stated that the users bear all the risks, 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 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,

---

2 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).

3 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’. 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 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:

- 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
- 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:

- 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
- 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.

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

© 2019 Law Business Research Ltd
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, the Portuguese Tax Authority (PTA) recently issued binding rulings stating that transactions, such as exchange of cryptocurrency for traditional currency, and vice versa, should be exempt from VAT.

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, 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 ruling 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.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Protection of fintech technology can take place by 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, which are included in the Industrial Property Code – approved by Decree-Law No. 110/2018, of 10 December – have been subject to considerable revision and expansion, which is mostly related to 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. The Directive brought substantial changes to the trade secrecy regime, notably on the protection criteria and the enforcement regime, which is expected to become clearer and more effective with the mentioned legislative change.

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 General Data Protection Regulation (GDPR) (EU Regulation No. 2016/679, of 27 April). 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 general, the processing of personal data requires 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 bank 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 bank secrecy (including cross-border transfers) is permitted only with prior customer consent or if the processing is necessary to obtain one of the following:

\[ a \] compliance with a legal obligation to which the data controller is subject;
\[ b \] the pursuit of the legitimate interests of the data controller or the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests of the data subject; or
\[ c \] the performance of a task carried out in the public interest.
In the past, the Portuguese Data Protection Authority had already ruled in a specific case that all personal data processed by a bank is subject to bank 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.

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, including profiling. Lastly, there are 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.

Without prejudice to the above, Portuguese legislation implementing or densifying the GDPR is currently in preparation and may bring some additional adjustments or restrictions to the rules set out in the GDPR, notably concerning additional safeguards regarding the processing of financial data. The CNPD has consistently ruled that financial data are sensitive data, in the sense that they reveal aspects of an individual private life and, thus, said data should be protected under the Portuguese Constitution. This may prove influential in the final version of the Portuguese data protection implementing act and may affect fintech companies operating in Portugal or offering services to Portuguese customers.

**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 is also beginning to take its first steps, with new platforms being registered and others in the middle of the registration and authorisation procedures, which boosts the fintech market in this area.

IX OUTLOOK AND CONCLUSIONS

The newly 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 PISP 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’ 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.

The Portuguese fintech market, which has observed a rather slow but steady development, shall greatly benefit from the PSD2 innovations. 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 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 million citizens and a high internet penetration rate of 73 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 with and data about their customers. For example, the largest banks are building their own financial marketplaces and their own 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 & Partners.
2 https://www.cbr.ru/eng/.
3 Information in English available at: https://finopolis.ru/en/.
II REGULATION

i Licensing and marketing

‘Fintech’ is an umbrella term that includes several different business models ranging from traditional payments and collective investments to novel areas, such 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. As of 2013, the powers of the Central Bank also extend over the issuance of securities and exchanges, which were previously supervised by the Federal Financial Markets Service (now defunct), thus making the Central Bank the ultimate authority in 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:

a the Ministry of Finance is responsible for general financial policy and for overall management in the field of finance in Russia;

b 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;

c the Federal Financial Monitoring Service (Rosfinmonitoring) is mainly tasked with anti-money laundering (AML) and counter-terrorism financing functions; and

d 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 9 February 2018, there are 21 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

---

⁶ See footnote 4.
⁷ https://racib.com/.
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, the Federal Law on Consumer Protection.⁹

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 2018, there are 17 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 most often leads to the 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, despite the fact that 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 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 66 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. At this stage, customers may only use UBS to open a bank account with a few banks. However, 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, FUNDING AND PAYMENT SERVICES

i 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.

ii Automated digital advisory services or ‘robo-advisers’

Until recently, digital advisers (also known as ‘robo-advisers’) have been beyond regulatory reach. In fact, there were no requirements applicable to investment advisers at all. This changed in late 2017, with the adoption of amendments into the Federal Law on Securities Market, according to which there will be a new type of professional market participant, namely investment advisers. The same amendment law states that if investment advice is provided by means of software, including via internet, such software shall be accredited by the Central Bank. This provision is interpreted to include robo-advisers within the scope of regulations that will be broadly applicable to investment advisers. The law came into force on 21 December 2018.

Investment advisers must be registered with the Central Bank and be members of one of the relevant SROs. SROs for investment advisers shall develop basic standards, setting out more detailed regulations for their members. The basic standards for investment advisers are yet to be developed.

iii Crowdfunding and crowd investing

For the sake of this chapter, we will differentiate between the two concepts. Crowdfunding generally refers to cases where a broad community supports a project in exchange for symbolic tokens (perks) or future products (presale). By its very nature, crowdfunding is less risky and usually subject to less oversight from regulators. In Russia, it is not subject to any specific regulations. There are several platforms on the Russian market that let companies or groups of individuals raise funds in the form of donations or presale orders.

In contrast to crowdfunding, crowd investing implies that there is an investment interest (i.e., participants expect to receive profits from the success of a project, and such profits may vary or be non-existent). In the context of crowd investing, investee companies usually offer some sort of an interest in their capital or cash flow, be it a participation interest in an LLC, shares of stock in a joint-stock company or units in an investment fund. Transactions with all these instruments under Russian law require the physical presence of a purchaser, which is one of the obstacles to the widespread introduction of crowd investing. In fact, the only model that proved viable in these circumstances is online-to-offline, where investment opportunities are marketed online and actual transactions are entered into offline. At the moment, such platforms themselves are not subject to any licensing requirements, nor are they bound by a duty of care or loyalty to prospective investors. This is likely to change with the introduction of a legal framework for crowd investing, which has been proposed by the Central Bank (covered below).

iv Crowd or peer-to-peer lending

There is no special legal framework for crowd lending (also known as peer-to-peer lending). In 2016, in its analysis of the peer-to-peer lending market, the Central Bank acknowledged that ‘Russia fits the unregulated market model, since no definition of this type of activity exists in the legislation and there is no special regulation.’\textsuperscript{15} Despite this fact, a lot of peer-to-peer lending platforms on the market (but not all) are registered as microfinancing organisations (covered in more detail below), which allows them to extend loans themselves, instead of just bringing individual borrowers and lenders together on an online platform.

It is contemplated that certain regulations for peer-to-peer lending will be adopted soon. In fact, the Central Bank has already initiated discussions among market participants, created a working group and invited various platforms to submit certain reports on a voluntary basis.

Apart from peer-to-peer lending model, there is also a growing market for peer-to-business (P2B) lending, where individuals may extend loans to companies. Notably, such P2B-lending platforms operate despite the restriction set forth in Article 807(4) of the Russian Civil Code that explicitly prevents companies from raising public debt unless by means of a regulated bond offering or in other cases specifically set forth in the law.\textsuperscript{16}

v Microfinancing

As mentioned above, some platforms combine activities of pure peer-to-peer lending (serving as a marketplace for individual borrowers and lenders) and microcredit (extending loans). In fact, the microfinancing industry (bearing similarities to what are known as ‘payday loans’ in the United States) is a big industry in Russia, with 2,007 microfinancing organisations (MFOs) registered with the Central Bank as of December 2018. The status of an MFO is required for an organisation to be able to extend loans on a regular basis (without being required to obtain a full-scale banking licence).

There are two types of MFOs: microcredit companies (MCCs) and microfinancing companies (MFCs). MCCs are not subject to capital requirements, but also limited in their sources of funding and the size of loans they may extend. MFCs must have at least 70 million roubles in their own capital but may also extend bigger loans and issue bonds. Despite the large number of MCCs, the market is dominated by MFCs that collectively account for 55.6 per cent of the total consumer loan book of 133.7 billion roubles as of the end of Q2 2018.\textsuperscript{17}

In the context of the growing segment of digital lending, since 2015, MFOs may issue loans of less than 15,000 roubles per one borrower with the means of remote ‘simplified identification’, which allows for full digital onboarding subject to certain rules.

Similar to other jurisdictions, interest rates for consumer loans are capped in Russia. Specifically, the full value of a consumer loan may not exceed by more than one-third of the weighted average interest rate calculated by the Central Bank on a quarterly basis for particular types of loan.


\textsuperscript{16} For instance, see Article 9(1)(1) of the Federal Law No. 151-FZ on Microfinancing Activities and Microfinancing Companies dated 2 July 2010, which allows microfinancing companies to raise public debt under certain conditions.

vi Payment services

Payment services is a regulated activity in Russia. The main piece of legislation is the Federal Law on the National Payment System (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 2019, there were 33 active payment systems listed in the register maintained by the Central Bank.

vii 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 subject to such obligation.

V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

As early as 2014, various regulators in Russia for the first time acknowledged the existence of bitcoin by demonstrating their negative views towards it. This even culminated in a bill proposed to introduce criminal liability for transactions with bitcoin in 2015. The bill was never adopted and since then the overall position has changed. In 2017, the attitude of regulators towards bitcoin shifted from ‘banned, unrecommended’ to ‘the concept is under investigation, regulation will come soon.’

In the absence of any specific laws or regulations, experts tend to classify bitcoin and other cryptocurrencies as property, as opposed to currency, since the only lawful means of payment in the territory of Russia is the rouble. According to the Federal Tax Service, there is no ban on the use of cryptocurrencies in Russian legislation, and general taxation principles shall apply to mining and transactions with cryptocurrency transactions.

When it comes to tokens and ICOs, there is relatively less clarity. In September 2017, the Central Bank warned investors of the risks inherent to ICOs, but apart from that no other regulator or court has yet had a chance to investigate the legal nature of tokens. Despite this fact, ICOs in Russia gained significant traction in 2017, which was likely driven by restricted access to venture capital for early-stage projects. It is estimated that projects with Russian founders raised approximately US$310 million in 2017, thus occupying the second position in the total ranking between the United States and Singapore. Notably, most of these ICOs have been structured through entities in foreign jurisdictions, not in Russia.

In this context, experts tend to agree that all tokens are different. They may represent various underlying rights or assets, and thus should be treated according to their substance.

---

19 Available in Russian at: www.cbr.ru/PSystem/rops/.
rather than form. Arguably, it is more important to introduce an efficient legal framework for crowdfunding, thereby allowing retail investors to support new ventures, instead of regulating technological aspects of tokens. Following this logic, in January 2018, the Central Bank came up with a proposal to introduce crowdfunding in Russia. Under the proposed bill, companies will be able to issue ‘tokens’ that will serve as instruments of record for various property rights (see Section IX below).

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, 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 a 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 on 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.

**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**

While there is no specific regulation applicable to smart contracts, this topic has been widely discussed among both legal and finance professionals in 2017–2018. Moreover, several banks and industry groups announced initiatives to implement smart-contract functionality in their systems. Among such initiatives is Masterchain, which is an Ethereum-based blockchain developed by the consortium of major Russian banks cooperating within the Association for Financial Technologies Development. Masterchain claims to be the first blockchain in

---


Russia to satisfy the requirements of applicable law, thus making smart contracts entered into and executed thereby legally binding. 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.26

At the same time, there is still an ongoing discussion about whether smart contracts really represent a new contractual paradigm or rather such contracts are a more efficient way to execute traditional contracts.

ii Automated digital advisery

As discussed above (see Section IV), since December 2018, automated digital advisory services (robo-advisers) are now 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 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.

iv 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 INTELLECTUAL 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.

---

26 Masterchain’s whitepaper is available in English at: http://fintechru.org/documents/Masterchain_whitepaper_v1.1_en.pdf.
Rights over trademarks are granted by virtue of registration with Rospatent,27 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.28 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 creation of IP falls within the duties of an employee.

ii Data protection

Overall, Russian data protection law is in line with international standards. In fact, 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 Data29 and the Federal Law on Information, Information Technologies, and Data Protection.30

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

While the main topic in 2017 was crypto and ICO, the fintech agenda in Russia in 2018 was more focused on developing the legal framework for the digital era of finance. Specifically, there are three bills under consideration in the State Duma, the lower chamber of the Russian parliament, aimed at laying the foundation for digital assets and crowdfunding. It remains to be seen whether these laws will eventually be adopted, as some experts suspect that the introduction of these bills was a reactionary response to the cryptocurrency market hype in 2017.

Another topic that has started gaining traction at the end of 2018 relates to the fees charged by acquiring banks from the merchants (retailers). President Putin named an as high as 3 per cent fee charged by banks a ‘quasi-tax’, following which the Federal Anti-Monopoly Services initiated an investigation, sending out information requests to major banks and retailers.

Apart from the above changes, the past 18 months were relatively stable and there were no major fintech regulations that became binding law. In the previous edition, we discussed that in 2017 the Russian government has adopted an extensive action plan aiming

28 Madrid Agreement Concerning the International Registration of Marks of 1983.
to introduce normative regulation of the digital economy that, among other things, includes many areas that will directly impact fintech.\textsuperscript{31} So far, the contemplated measures are still under development and subject to discussion with the expert community.

**IX OUTLOOK AND CONCLUSIONS**

We expect 2019 to be driven by the agenda set at the end of 2018. Specifically, we expect the Central Bank to move forward with rolling out the system of fast intra-bank payments. This measure aims to lower the dependence of Russian banks on international payment systems.

Further, we expect that SROs for various participants on the securities market will carry out their mandates and adopt basic standards governing the specifics of particular financial services and products.

In addition to that, we will likely see more bills and supporting legislation being introduced within the framework of the digital economy action plan.

\textsuperscript{31} Action Plan 'Normative Regulation' within the programme 'Digital Economy of the Russian Federation', as adopted by the Government Commission on the Use of Information Technologies for Life Quality and Business Environment Improvement on 18 December 2017. Available at: http://static.government.ru/media/files/P7L0vHUjwVJPlNhM2qZQqEeVqXACwXR.pdf.
Chapter 21

SINGAPORE

Adrian Ang V-Meng and Alexander Yap Wei-Ming

I OVERVIEW

Over the course of the past three to four years, the Singapore government and related statutory boards identified fintech as a potential 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, in August 2015, the Monetary Authority of Singapore (MAS) formed a Financial Technology and Innovation Group within MAS to drive such initiatives. 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 a ‘sandbox’ as a safe space 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:

a. the Technology Enterprise Commercialisation Scheme;

b. the Financial Sector Technology and Innovation (FSTI) scheme; and

c. 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.

Other Singapore government initiatives that aim to deepen know-how in fintech and related areas include:

a. AI.SG, a national programme to boost Singapore’s artificial intelligence capabilities, which will initially focus on finance, city management solutions and healthcare. The National Research Foundation is expected to invest up to S$150 million in AI.SG over the next five years;

b. Accreditation@SGD, through which the Info-Communications Media Development Authority independently evaluates Singapore-based technology product start-ups on whether their product functions in accordance with claims and provides an independent assessment of their ability to deliver, team, processes, and financial sustainability; and

1 Adrian Ang V-Meng and Alexander Yap Wei-Ming are partners at Allen & Gledhill LLP.
the Singapore Data Science Consortium, established as the key platform in Singapore for industry to access data science technologies, applications and expertise from academia.

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 International 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 operating a remittance business under the Money-changing and Remittance Business Act; and
regulatory requirements imposed on the operator of a ‘payment system’ or the holder of a ‘stored value facility’ under the Payment Systems (Oversight) 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. By way of example, a fintech company that operates a securities crowdfunding platform may 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 that reliance is placed on a specific prospectus registration exemption for such purposes and the invocation of such prospectus registration exemption carries with it advertising restrictions (i.e., restrictions on marketing the specific share). To use another example, an automated digital advisory or asset management company may be construed to be 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). Following on from this, the relevant licence granted to the fintech company may have a condition that restricts the dealings of such automated digital advisory or asset management companies to ‘sophisticated’ investors. Such a restriction would restrict the ability of the fintech company to market its services to retail investors.

ii 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 on the basis that it is licensed in such jurisdiction. As such, the offering of fintech products and services to persons in Singapore may trigger licensing requirements in Singapore on the part of the offeror, regardless of its licensing status in another jurisdiction. This will 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 have extraterritorial effect. In this regard, ‘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’. Where an act is done entirely outside of Singapore, licensing requirements would apply, where such conduct has a ‘substantial and reasonably foreseeable’ effect in Singapore. 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. The lack of marketing to persons in Singapore should be one of many factors to be considered.
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.

A new national digital identity (NDI) system is presently being developed by the GovTech as part of the Singapore Smart Nation initiative, and it is expected to become operational in 2020. It is reported that GovTech will work with the private sector to develop services that make use of the NDI, which 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, FUNDING AND PAYMENT SERVICES

The marketing and management of collective investment schemes, 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 AND INITIAL COIN OFFERINGS

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.

MAS has indicated in a statement released on 1 August 2017 that the offer or issue of digital tokens in Singapore will be regulated by MAS if the digital tokens constitute products regulated under the SFA. 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 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 fulfil 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

---

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,
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
analysis. 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 artificial intelligence 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 the Intellectual Property Office
of Singapore 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.

---

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'.
4 'Information' includes 'data, text, images, sound, codes, computer programs, software and databases'.
5 Section 11 of the ETA.
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:

a. 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

b. 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:

a. confidential as regards the giver of the data or information; and

b. 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 banking secrecy and trust secrecy regimes. 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.
The Payment Services Act has not, however, come into effect. Once the Act comes into effect, it may be the case that there may be more 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 to 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).
Chapter 22

SPAIN

Leticia López-Lapuente and Isabel Aguilar Alonso

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 337 as at February 2019.

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,

1 Leticia López-Lapuente is a partner and Isabel Aguilar Alonso is a counsel at Uría Menéndez.
2 Source: finnovating.com.
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, in July 2018, the Spanish Ministry of Economy and Business published the Draft Law for the Digital Transformation of the Financial System (the Draft Bill), which was discussed by the Spanish government in February 2019. The final text of the Draft Bill is not public at the moment; however, it is known that the purposes of such Draft Bill are:

a ensuring that financial supervisory authorities have adequate instruments to keep performing their supervisory and regulatory functions within the new digital environment; and

b facilitating the innovative process 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 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 services 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, FUNDING AND PAYMENT SERVICES

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:

a 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;
b the transferor must disclose in its annual reports the current and future assignment of credit rights that impact each year;
c the assignment of the assets to the fund should be formalised in a contract; and
d 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 AND INITIAL COIN OFFERINGS

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 the ESMA.
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 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-resident taxpayers 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 a type of cryptocurrency for another cryptocurrency) 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;

b 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;

c 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 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.

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 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:

a. Spanish patents provide protection for inventions for 20 years as of the filing date;

b. utility models protect inventions of lower inventive rank than patents, and are granted for a period of 10 years;

c. once the referred protection periods have expired, the invention will enter the public domain and may be freely used by any person; and

d. know-how and trade secrets have value as long as they are kept confidential, as opposed to patents, and therefore it is a matter of contract (confidentiality agreements) and of fact (other protective measures adopted) that the invention remains valuable.

On a separate note, software would not be deemed an invention but would be 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):

a. 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

b. 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. 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.3

---

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:

a) host an EU FinTech Laboratory where European and national authorities will engage with tech providers in a neutral, non-commercial space;

b) present a blueprint with best practices on regulatory sandboxes, based on guidance from European Supervisory Authorities; and

c) 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.

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.
Spain

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.
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 and financial institutions to experiment with new business models. 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 an equally comprehensive proposal for focused changes to existing laws published on 22 March 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. Regular updates on developments are available on a (private) site.

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 Stock Exchange Act (SESTA, to be abolished by the Financial Institutions Act by 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 great 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/.

© 2019 Law Business Research Ltd
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 as a very fintech-friendly jurisdiction, despite the fact that no fintech specific regulation or tax regime exists. Many fintech startups and projects show that the legal environment is considered as advantageous. Currently, the main impediment for fintech projects in the field of cryptoassets is 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.

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 SESTA 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:

\begin{itemize}
\item[a] the funds do not at any time exceed 1 million Swiss francs;
\item[b] the funds are neither reinvested nor interest-bearing (with exceptions); and
\item[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.
\end{itemize}

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.\(^6\)

**SESTA**

A licence from FINMA is required in order to act as securities dealer.\(^7\) A securities dealer 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:

\begin{quote}
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.
\end{quote}

Therefore, for trading tokens it is relevant whether these are qualified as securities within the meaning of SESTA (see below, on ICOs). The SESTA will be abolished on 1 January 2020, with the coming into force of the new Financial Institutions Act. Securities traders will be renamed securities houses, but the general regulatory framework applicable to them is not expected to change much.

\(^5\) Article 5 Paragraph 3 Lit. c Banking Ordinance.
\(^6\) Article 1a and 1b Banking Act.
\(^7\) Article 10 Paragraph 1 SESTA.
\(^8\) Article 2 Lit. d SESTA.
**AMLA**

Even if neither a banking nor a securities dealer’s 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 dealers, 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.

**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 in Switzerland, the same licence requirements would apply as for any other institution offering non-digital advisory services. At the current stage, a ‘pure’ investment advisory without any power of attorney over client’s accounts is not subject to licence requirements (but will become subject to behavioural rules similar to the Markets in Financial Instruments Directive by 2020). Investment advisory with a power of attorney is not subject to a licence requirement; however, the institution will be required to subject itself to the supervision of an AML SRO (or alternatively directly to supervision by FINMA).

Credit information services may be provided subject to the FADP; under 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.

**Financial Services Act and Financial Institutions Act**

In 2020, the Financial Institutions Act (FinIA) and the Financial Services Act (FinSA) are expected to enter into force simultaneously, and they will bring major changes to the regulation of the Swiss financial market.

**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 today’s rules, however, cross-border inbound marketing of banking products, as a rule, does not require a licence (but will subject the marketing company to the new FinSA rules from 1 January 2020).

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, FUNDING AND PAYMENT SERVICES

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.9 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, SESTA, AMLA, etc. In addition, a consumer credit agreement is a contract whereby a creditor grants or promises to grant credit to a consumer in the form of a deferred payment, a loan or other similar financial accommodation.10 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.11

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.\(^\text{12}\) 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,\(^\text{13}\) provide for a guarantee of irrepachable business conduct,\(^\text{14}\) the minimum capital of the applicant must be fully paid in\(^\text{15}\) and the applicant must possess appropriate IT systems.\(^\text{16}\)

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 CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

Switzerland does not 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 particular the ‘Crypto Valley’ in the canton of Zug established itself as one of the world’s hubs for ICOs, in particular through the Etherum 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

\(^\text{12}\) Article 4 FMIA.
\(^\text{13}\) Article 8 FMIA.
\(^\text{14}\) Article 9 FMIA.
\(^\text{15}\) Article 12 FMIA.
\(^\text{16}\) Article 14 FMIA.
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.

A key message given by the ICO Guidelines is that FINMA continues to be ready to review ICOs 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 under the Swiss Code of Obligations.

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 recently 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 (AML) 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.

---

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. The minimum standard entails providing information on technical features, financial situation, the management team involved and the involved risks and respective compliance procedures (e.g., KYC process). In addition, members should ensure that pre-deployment and deployment are audited by an independent auditor. It is not yet certain whether these standards will all prevail. 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.

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.

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

18 Article 5 Lit. c UCA.
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 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:

- the controller of the data file;
- the purpose of the processing; and
- 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.

**VIII YEAR IN REVIEW**

The past 18 months were an intense phase for Swiss fintech regulations.

In January 2018, the Swiss State Secretariat for International Financial Matters established a blockchain/ICO working group. Also in January 2018, the private Crypto Valley Associations proposed a first Swiss Code of Conduct for ICOs, proposing detailed and extensive information requirements for enterprises conducting an ICO and suggesting that each stage of an ICO be independently audited. On 16 February 2018, FINMA published its Guidelines for ICOs, providing a regulatory framework to classify tokens and giving indications as to their treatment under AML laws. Furthermore, several cantonal tax administrations issued guidelines on how they will assess bitcoins for tax purposes.

While the ICO boom of 2017 slowed down considerably, in 2018 infrastructure projects (crypto-brokers, trading places, wallet and storage providers) started to dominate the scene. In June 2018, the first Swiss crypto-trading place SCX took up operations.
On 21 September 2018, the Swiss Bankers Association Guidelines on opening corporate accounts for blockchain companies were published. As various projects had problems finding a bank that was willing to open a corporate account, in particular to accept the proceeds of an ICO, this was a welcome confirmation of the industry’s support for the new fintech sector. In October 2018, a report of the interdepartmental coordination-group to fight money laundering and terrorism financing was published and found that, up to the date of the report, no cases of money laundering by way of using cryptoassets in Switzerland has become known. The report was cautious about strengthening the AML rules, as Swiss AML rules already cover more aspects than, for example, EU rules. However, the national platform Cyberboard, bringing together law enforcement officials from all over Switzerland, was considered to be an important tool. In the revised Finma-AML-Ordinance (changes as of 20 June 2018), additional duties of review were introduced for issuers of means of payment (such as payment tokens); the revised ordinance is expected to become effective on 1 January 2020.

In December 2018, the long-awaited report of the Swiss Federal Council, the Swiss government, on the legal basis for distributed ledger technology and blockchain in Switzerland, with a focus on applications cases in the finance sector, gave a comprehensive overview of the current legal regime and proposed changes to it. In summary, the report advocated not introducing a separate blockchain act, but rather to adapt existing laws to abolish certain aspects that may hinder the new technologies. A first proposal for such changes was published on 22 March 2019 (the Federal Act on adapting the Federal law to developments of the DLT). Interested parties may now send comments until summer 2019 and thereafter, the Federal Council will draft its formal proposal to parliament.

The draft focuses on security tokens which are to be regulated as intermediated securities under security law, debt enforcement law and international private law. Furthermore, a new financial market infrastructure is proposed, the ‘DLT trading system’, which may combine the functions of a trading platform, a depository and a payment system (but not as a central counterparty).

**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 in a final form by the end of 2019.

The draft of the new Data Protection Act published in 2017 is still on hold. It is expected that it will not be discussed in parliament prior to the end of 2019 and will not become effective in 2020.

The first proposal of the Federal Act on adapting the Federal law to developments of distributed ledger technology (DLT) will be discussed in 2019 and it can be expected that a final proposal of the government will be submitted to parliament by the end of 2019.

Hence, while the changes to Federal law to better adapt it to DLT may take some time, there are numerous private and public initiatives that focus on establishing wallet providers, trading platforms and various other projects 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 further announced that it intends to establish 18 new chairs for digitalisation topics. In addition, private promoters are about to establish sample standardised documents to further facilitate the use of the new technologies.
A focus in 2019 will clearly be on asset tokens; the first projects to tokenise shares and bonds are already operative, and it is hoped that this will enable small and medium-sized companies to tap the international financial markets much more efficiently. At the same time, there are various insurtech projects, projects to facilitate client onboarding (regtech) and projects to use artificial intelligence in the financial sector. Hence, even though the ‘crypto boom’ of 2017 may be over, the future has only started for the Swiss financial industry and the environment will remain very dynamic and can also count on continued support by the Swiss and Cantonal governments.
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:

\[ a \] there should be a periodical review of the algorithm;
\[ b \] relevant know-your-customer procedures should be conducted before provision of advice;
\[ c \] a special committee should be established to supervise the adequacy of the Robo-Adviser Services; and
\[ d \] 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.

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, FUNDING AND PAYMENT SERVICES

i 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 after 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.

ii 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.

iii 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.
iv Loans trading

The general principle under Taiwan’s Civil Code is that any receivable is assignable unless:

a the nature of the receivable does not permit such transfer;
b the parties to the loan have agreed that the receivable shall not be transferred; or
c 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.

v 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:

a collecting and making payments for real transactions as an agent;
b accepting deposits of funds as stored value funds; and

c 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 AND INITIAL COIN OFFERINGS

As of the date of this article, there are 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.

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 as 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
Taiwan

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

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.

The term 'securities' has a very broad (but maybe not clear enough) definition in Taiwan. According to Article 6 of the SEA, ‘securities’ could mean government bonds, corporate stocks, corporate bonds and other securities approved by the competent authority, and any stock warrant certificate, certificate of entitlement to new shares and certificate of payment or document of title representing any of the above securities shall be deemed securities. Additionally, according to a recent Taiwan Supreme Court opinion, a contract or agreement would be considered as a security under the SEA if it has monetary value, the nature of an investment and transferability.

According to a news report in October 2018, the Chairman of FSC, Willington Koo, advised that the FSC will announce relevant new regulations governing offering of tokens with natures in securities (STOs) in June 2019.

ii Anti-money laundering

It was also 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 models should be examined on a case-by-case basis. Take self-executing contracts (i.e., smart contracts based on blockchain technology) for example. As mentioned above, as at the time of writing, no laws or regulations have been specifically promulgated or amended as a result of blockchain technology (including smart contracts). However, as a general rule, in Taiwan, general contracts can be formed by a meeting of the minds, and these can be expressed and proven by way of electronic records, unless otherwise provided by law. For example, under current law and practice, it is not feasible to structure a contract under which the relevant obligations will be automatically performed (when relevant conditions precedent are met) by electronic means when it comes to, for example, the creation of a valid mortgage over real estate or pledge over shares with physical certificate. Additional legal formality will be required and can only be fulfilled physically.

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 Regulatory sandbox

As advised in Section I, the Sandbox Act has been in effect since 30 April 2018. The enforcement rules for the regulatory sandbox were further promulgated by the FSC in April 2018.

According to the Sandbox Act, an applicant needs to obtain approval from the FSC before entering the sandbox. Once approved, the experimental activities may enjoy exemptions from certain laws and regulations (such as FSC licensing requirements and certain legal liability exemptions). According to the Sandbox Act, any experimental activity needs to be ‘innovative’. After completion of the approved experiments, the FSC will analyse the results of the experiments. If the result is positive, the FSC would actively examine the existing financial laws and regulations to explore the possibility of amending them so that the business model or activity previously tested in the sandbox could become legally feasible.

At the time of writing, three applications for entering the sandbox were approved, including one bank’s application for an online credit card business credit loan and two companies’ applications for cross-border remittance for foreign workers.

ii Digital-only banks

In 2018, the FSC promulgated relevant regulations governing the application for establishment of digital-only banks (i.e., banks without physical branches). According to the FSC’s press release and relevant news report, the deadline for digital-only bank applications
was 15 February 2019, and three applications were filed with the FSC by this deadline. According to the FSC, it will only approve two applications, and the result will be announced by June 2019. Once approved, a digital-only bank will be subject to the same requirement for paid-in capital as ordinary commercial banks, which is NT$10 billion.

IX OUTLOOK AND CONCLUSIONS

i Virtual currencies or cryptocurrencies, exchange operators and ICOs
The governance of cryptocurrency transactions, exchange operators and ICOs is a trending topic in Taiwan, and several public hearings and seminars were held to discuss this. Some suggested that the regulators and legislators should enact a new law to specifically regulate the exchange operators, but others proposed to establish a self-disciplinary organisation to set out relevant self-disciplinary rules for cryptocurrency-related activities, including ICOs. The most recent development is that, as advised above, the FSC, according to Mr Koo, will announce relevant new regulations governing offering of STOs in June 2019. However, the scope of such new regulations (e.g., whether the regulations will cover not only the primary market (i.e., offering) but also the secondary market (i.e., trading)) is still uncertain.

ii Regulatory sandbox
According to a press release issued by the EY in 2018, regulators expect to process at least 10 applications for financial innovation experimentation each year for the next three years. With three approved experiments in the regulatory sandbox, as mentioned above, we foresee more applications to come.
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), 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 Financial Conduct Authority (FCA), which maintains a reputation as one of the gold standard regulatory bodies worldwide, applying the UK’s existing regulations without additional requirements (save in the context of the regulated activities created following the implementation of the Payment Services Directive and the Revised Payment Services Directive) while participating in national and international sandboxes. UK regulation is likely to change over the coming years, as Parliament and the regulators grapple with the regulation of cryptoassets and virtual currencies.

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. 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 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 fintech business relate to the provision of payment services then the regime implemented in the Payment Services Regulations 2017 (PSR) will apply instead of the Financial Services and Markets Act (FSMA) to the authorisation, registration and conduct of business obligations of those businesses. These aspects are discussed in more detail in Section IV.

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.
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 the Prudential Regulation Authority (PRA). 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 for fintech businesses. 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 that allows those firms to operate in a limited manner under the close supervision of the FCA. As 2018 ended, the application deadline passed for the fifth cohort of the sandbox.

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. Breach of this restriction on financial promotions carries 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 made.

---

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.
This is a structure often implemented in crowdfunding, for example, where the business seeking equity investment through the 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 the business of a fintech does not involve it carrying 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 without needing to rely on any passporting mechanism.

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.

For those that are based in Europe, there is a complex web of EU passporting regimes that may apply depending on the activities carried on by the fintech. For example, electronic money institutions may passport under the Second Electronic Money Directive,16 while fintechs that provide insurance intermediary services may use the regime under the Insurance Distribution Directive.17 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)18 and Payment Services Directive (PSD2). Of course, this is complicated at present by the uncertainty surrounding the UK’s withdrawal from the EU.

Those firms outside the EU looking to provide similar services in the UK will not benefit from the passporting arrangements (to the extent they would apply to EU-based firms) and will need to seek separate authorisation.

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.

---

16 2009/110/EC.
17 (EU) 2016/97.
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, FUNDING AND PAYMENT SERVICES

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 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.

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.

---

19 CP18/20, which closed in October 2018 with a final policy statement due in Q2 2019.
Payment services

The payment services caught by the PSRs 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). These were newly defined regulated activities in 2017 and are intended to capture those businesses that look to utilise open banking standards to provide consumers with detail about their financial position by taking information directly from their banking providers, 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),20 small electronic money institutions (EMIs)21 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.

V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

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 in the UK. 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. The UK has not yet implemented any specific cryptoasset laws or regulations, and cryptocurrencies are, therefore, not currently regulated by the FCA provided that they are not part of other regulated products or services. This is not the case for cryptocurrency derivatives (i.e., cryptocurrencies that have the same properties as traditional derivative contracts), because these will be treated as derivatives and, therefore, specified investments for the purposes of the regulations. As a result, dealing in, arranging transactions

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.
in, advising on or providing other services that amount to regulated activities in relation to derivatives that reference either cryptocurrencies or tokens issues through an initial coin offering (ICO) will require authorisation by the FCA.

The above position is not likely to remain the same for very long because in January 2019 the FCA launched a consultation\(^{22}\) that builds on the work of the UK Cryptoassets Taskforce and the FCA to consider where different types of cryptoassets might fall in the regulatory perimeter. In short, this consultation proposes that cryptoassets be sorted into three categories:

\(a\) Exchange tokens:
- not issued or backed by any central authority and intended and designed to be used as a means of exchange;
- usually a decentralised tool for buying and selling goods and services without traditional intermediaries; and
- usually outside the regulatory perimeter.

\(b\) Security tokens:
- with specific characteristics that mean they meet the definition of a specified investment (see above) like a share or a debt instrument; and
- within the regulatory perimeter.

\(c\) Utility tokens:
- grant holders access to a current or prospective product or service but do not grant holders rights that are the same as those granted by specified investments; and
- although not specified investments, utility tokens may meet the definition of e-money in certain circumstances (as could other tokens), in which case they would be within the regulatory perimeter.

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, one of the proposed outcomes of the FCA’s current consultation on cryptoassets is for HM Treasury to consult in 2019 on the transposition of the EU’s Fifth Anti-Money Laundering Directive into UK legislation and to broaden the Anti-Money Laundering/Counter Terrorist Financing Regulation further in relation to cryptoassets.

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, some clarification was needed, as HMRC’s 2014 guidance focused mainly on certain types of cryptocurrency and was very limited in scope. HMRC has therefore produced revised guidance, covering the tax treatment of cryptoassets for individuals and where these are used as a form of employee reward. Unfortunately, there has so far been no clarification 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.

\(^{22}\) CP19/3: Guidance on Cryptoassets.
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. The most recently 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 as 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,23 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.


© 2019 Law Business Research Ltd
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.

---


25 The organisation that originates the contents of the database does not get the benefit of the protection as they do not need to expend time finding, checking and verifying the contents (since they originated the contents). Clearly, the key is investment in collection rather than creation of the content.
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.

VIII YEAR IN REVIEW

The year 2018 began with the deadline for national governments to transpose PSD2 into local legislation and for the largest UK banks to make personal and business current accounts data available through open application programming interfaces to facilitate open banking. These two events were the beginning of a year in which the UK payments industry took centre stage, and a new brand of payment initiation and account information service providers became operational under the new rules.

The past year was also transformational for cryptoassets. January 2018 saw an unprecedented level of interest in the launch of new tokens and cryptocurrencies as the existing UK regulatory perimeter creaked at the edges under the pressure of trying to capture as many different features and concepts as possible. Since then, the FCA started to take a clearer and more robust stance on its interpretation of the existing regulations, before commencing a formal consultation on a bespoke regime for cryptoassets that clearly delineated between the three types of cryptoasset detailed in Section V.

MiFID II also came into effect in the UK on 3 January 2018. It includes a broad spectrum of measures covering everything from data reporting28 and transparency to client

26 ICO Big data, artificial intelligence, machine learning and data protection report 2017.
28 This was augmented by the coming into force of the General Data Protection Regulation on 25 May 2018, which caused some consternation among firms trying to marry the two regimes.
categorisation. It has also been used in the latter part of 2018 as a basis of European-level thinking for the regulation on cryptoassets following the publication of a report by the European Securities and Markets Authority’s stakeholder group on how to address the risks of ICOs. The rules have directly affected those fintech businesses deemed to be carrying on ‘MiFID business’ (i.e., (1) investment services and activities and (2) ancillary services carried on by a MiFID investment firm). MiFID’s copious data-reporting obligations also boosted those fintech firms operating in the regtech sphere, as a number of financial services businesses sought to outsource compliance with the complex and copious rules to third-party technology providers.

IX OUTLOOK AND CONCLUSIONS

Much of the focus in the coming months will be on the outcome of Brexit and how it affects the market based on the deal (or lack of it) reached with the remaining EU Member States.

Currently, in a ‘no deal’ scenario, UK passporting rights will immediately cease to exist but, at the time of writing, the FCA is working on its no-deal planning including by proposing a temporary permissions regime for firms looking to operate in the UK from the EEA. Meanwhile, if the UK secures consent for a withdrawal agreement then, when it leaves the EU after the transitional 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, even in the event of a no deal, those rules will be transposed into the UK statute book so as to continue to be effective.

One of the continuing regulatory changes that will take full effect in the UK in 2019 (irrespective of the outcome of Brexit) is the Senior Managers and Certification Regime, which has been slowly replacing the Approved Persons regime for authorised firms. Any fintech carrying on regulated activities will need to consider these new rules, which were extended to insurers in December 2018 and will take effect for all firms regulated by the FCA in December 2019.

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 UK has left, 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.29

29 Intellectual Property (Amendment) (EU Exit) Regulations 2018 and various impact assessments published by the Regulatory Policy Committee (RPC).
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.

It is also likely that clarification of the tax treatment of ICOs and initial token offerings will be forthcoming during 2019.
I OVERVIEW

Fintech covers a wide swathe of activities and businesses in the United States, but the common feature is the use of new technology to innovate the delivery of financial services to customers or to make the way financial services are processed more efficient and swift.

The US government and regulators are still in the process of determining how fintech activities and firms should be regulated, which is playing out on both the federal and state levels. While the US government and regulators are broadly supportive of fintech companies, there are currently few dispensations or programmes for fintech firms, and, if anything, fintech firms and activities have been subject to similar regulation and enforcement actions as traditional financial services companies, such as anti-money laundering regulations and anti-fraud and anti-manipulation laws and regulations.

Among the federal regulators, some or all of the US Securities and Exchange Commission (SEC), the Commodities Futures Trading Commission (CFTC), and the banking regulators, including the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation, have input into and have laid claim to license and regulate various fintech activities and firms. At the state level, the state regulators of financial services, including the New York Department of Financial Services, and the state attorneys general, have also voiced their expectations and concerns about fintech developments and regulation. In the meantime, regulated financial institutions, such as banks, that partner with fintech companies, are subject to existing regulations that limit their investments and subject their arrangements to regulatory scrutiny.

We expect continued developments on the issue of regulation and jurisdiction as the policymakers, regulators and the courts grapple with these issues. For example, the US Department of the Treasury has assembled a working group involving the SEC, the CFTC, the Board of Governors of the Federal Reserve System (Federal Reserve Board), and the Financial Crimes Enforcement Network (FinCEN), a bureau of the US Department of Treasury, to discuss jurisdiction over cryptocurrencies among the agencies, and to understand where gaps exist and whether a new regulatory scheme is warranted. That working group could make recommendations that would influence regulation in this area.

1 Jordan Altman and Reena Agrawal Sahni are partners at Shearman & Sterling. The authors would like to thank Mark Elzweig, Sean Anderson and Eli Kozminsky, all associates at Shearman & Sterling, for their assistance in preparing this chapter.
II REGULATION

i Licensing and marketing

Fintech businesses in the United States are not subject to a fintech-specific regulatory framework by any single federal or state regulator. Rather, depending on the activities of a fintech company, that fintech company may be subject to myriad federal and state laws and regulations, including licensing or registration requirements.

The number and complexity of potentially applicable US regulations to any single fintech firm has drawn some criticism as a potential barrier to entry and hindrance to growth of US fintech. As regulators work to develop regulations that govern the fintech space, there is also uncertainty as to precisely how the US regulation of fintech will evolve and the degree to which fintech companies will receive government support and collaboration as the industry develops.

Many fintech companies find that offering their services throughout the United States requires licensing and registration with multiple state regulators, subjecting such fintech companies to regulation and supervision by the laws and regulations of each such regulator. The types of licences that may be required at the state level include consumer lending, money transmission and virtual currency licences. Depending on the number of states and licences that are required to be obtained, a fintech company may find the compliance burden to be extensive as each state has its own distinct set of rules and regulations. There is currently a money services business licensing agreement between regulators in seven states, coordinated through the Conference of State Bank Supervisors, which standardises the elements of the licensing process and provides for recognition of other states’ reviews. There is also a CSBS model regulatory framework for state regulation of certain virtual currency activities, all of which are efforts to help overcome the challenges of licensing in 50 states.

On the federal level, the Consumer Financial Protection Bureau (CFPB) has jurisdiction over providers of financial services to consumers. Because many fintech businesses are aimed at providing services predominantly to consumers, the CFPB has the ability to enforce a range of consumer protection laws (such as consumer lending laws and anti-discrimination laws) that apply to the activities of such companies. The CFPB also has authority to enforce against the use of unfair and deceptive acts and practices generally.

To the extent that the activities of a fintech provider fall within the licensing regimes of other federal regulators, such as the SEC or the CFTC, such fintech providers will be required to register with such agencies and become subject to enforcement by the same. For example, robo-advisers, being a subset of investment advisers, may be subject to SEC registration requirements for such advisers. Finally, fintech companies may also be required to register with the US Department of Treasury’s Financial Crimes Enforcement Network (FinCEN) and thus, as described below, comply with the Bank Secrecy Act and other anti-money laundering laws and regulations.

The OCC, the primary federal bank regulator for national banks, previously announced that it will provide a special purpose national bank charter to fintech companies that receive deposits, pay checks or lend money. Fintech companies that choose to apply for and receive this special purpose national bank charter will become subject to the laws, regulations, reporting requirements and ongoing supervision that apply to national banks, and will also be held to the same standards of safety and soundness, fair access, and fair treatment of customers that apply to national banks. The OCC intends that, among other things, this special purpose national charter may help level the playing field between national banks and competing fintech companies, while also protecting consumers and providing greater...
consumer access to fintech services. The chartering of fintech companies by the OCC has drawn some criticism from state regulators, among others, who argue that the regulation of such companies is better accomplished at the local level by regulators who may have a deeper knowledge of certain fintech industry participants and more tailored regulations. In fact, the charter has been on hold in part because of lawsuits from certain state regulators that believe that an OCC charter exceeds the agency’s authority.

Regulators with jurisdiction over fintech businesses have not shied away from issuing enforcement actions where fintech businesses are conducting activities in violation of law. In recent years fintech companies have been subject to enforcement actions by regulators, including the CFPB, SEC and CFTC. Enforcement orders have been issued for, among other things, insufficient data security practices, violations of federal securities laws, including anti-fraud laws, failing to obtain requisite licences or registrations, and unfair and deceptive practices.

ii Cross-border issues

Even as financial services are increasingly provided across borders, the regulation of such financial services is still largely territorial. The regulation of financial services in the United States generally applies to firms offering services and products in the United States and to people in the United States, and so the same issues and regulations that apply to US fintech companies apply to non-US fintech services offered from abroad into the US jurisdiction. Broadly speaking, there is no passporting of regulated or licensed activities from outside the United States into the United States.

III DIGITAL IDENTITY AND ONBOARDING

There is no generally recognised digital identity in the United States at present, and no fully digitised onboarding of clients.

IV DIGITAL MARKETS, FUNDING AND PAYMENT SERVICES

The funding for fintech initiatives can come from a variety of sources that track traditional funding for new and growing businesses, including private equity funds and hedge funds, financial institutions, corporates, family offices and high net worth individuals. Such capital raises are used to both finance the company itself, and for lending purposes, where the company is engaged in lending activities.

i Crowdfunding

Crowdfunding, which generally refers to the use of the internet by small businesses to raise capital through limited investments from a large number of investors, is permitted under SEC rules and regulations. The Jumpstart Our Business Startups Act (the JOBS Act), established provisions that allow early-stage businesses to offer and sell securities, and the SEC subsequently adopted Regulation Crowdfunding to implement these provisions of the JOBS Act. The Financial Industry Regulatory Authority (FINRA) oversees the registration of crowdfunding portals. Broker-dealers and funding portals that are registered with the SEC and are FINRA members are permitted to offer and sell securities on behalf of issuers to the investing public using crowdfunding.
ii  Peer-to-peer lending

Peer-to-peer lending and crowd-lending are also permitted in the United States. Examples of peer-to-peer lending include Lending Club and Prosper. Online lending marketplaces often rely on bank partners to actually originate loans, and thereby rely on the licensing and regulation to which those banks are already subject. However, even such marketplaces are subject to a wide range of regulations, including state licensing statutes that can impose requirements relating to record keeping, servicing practices, disclosure requirements, examination requirements, surety bond and minimum net worth requirements, financial reporting requirements, change in control notification requirements, restrictions on advertising, and requirements regarding loan forms. Peer-to-peer lenders are also subject to consumer protection laws, including state usury limitations, state disclosure requirements and other substantive lending regulations, Truth in Lending Act disclosure requirements, Equal Credit Opportunity Act non-discrimination provisions, and Fair Credit Reporting Act, Fair Debt Collection Practices Act and CFPB regulations.

iii  Sales, transfers and securitisations

Such loans and financings can generally be traded on a secondary market, subject to certain limitations. So, for example, securities purchased in a crowdfunding transaction generally cannot be resold for a period of one year, unless the securities are transferred to the issuer of the securities, an accredited investor, as part of an offering registered with the SEC, or to a family member of the purchaser. Loans that are originated as part of peer-to-peer marketplaces can be subject to limits on the ability to ‘export’ the interest rate at origination upon a sale or transfer of the loan. Transfer to securitisation vehicles is not uncommon, and is generally subject to risk retention rules that require the securitiser or sponsor of the securitisation transaction to retain at least 5 per cent of the credit risk of the securitised assets.

iv  Payments services

Payments services are also subject to state licensing requirements. So, for example, states may license payment services as money transmitter businesses in the relevant states where money transmission services are provided. Such activities can also trigger registration requirements with FinCEN as a money services business. The board of governors of the Federal Reserve System has adopted Regulation E, which specified requirements for mobile banking or mobile payment transactions made via electronic fund transfers from a consumer’s asset account.

V  CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

There is currently no specific federal regulation of blockchain and distributed ledger technology (DLT), as the current regulatory framework consists mostly of guidance focused on the applications of such technology, such as cryptocurrency and initial coin offerings (ICOs). Many federal regulators have repeatedly spoken of the potential benefits of such technology, however, this optimism has not translated into any concrete rulemakings.

To date, almost all blockchain and DLT regulation has occurred at the state level. Some noteworthy legislation includes Delaware legalising the use of blockchain for the creation and maintenance of corporate records; Arizona amending its Electronic Transactions Act to affirm the validity of electronic signatures recorded on blockchains and permit the use of smart contracts; and Nevada banning local governments from taxing blockchain use.
Several federal and state regulators are also weighing blockchain and DLT legislation. The Commodity Futures Trading Commission’s Technology Advisory Committee recently voted to recommend the formation of subcommittees on DLT and cryptocurrency. Additionally, Illinois, North Dakota and Vermont have passed bills to create task forces to determine whether financial technology and blockchain regulation is necessary, and bills have been proposed in New York and Hawaii that would follow suit.

Through its investigative report of the decentralised autonomous organisation (DAO), the SEC determined that the organisation’s tokens were in fact securities, setting the precedent that issuers of digital tokens may be subject to SEC oversight and securities registration requirements. The report further states that whether or not a token is a security shall be determined on a facts-and-circumstances basis, and that the SEC will apply a multi-pronged test to determine if tokens are securities.

In the case of the DAO, the SEC found that investors had invested money in a common enterprise, had a reasonable expectation of profits from that investment and profits were derived from the managerial efforts of others. The SEC provided additional clarification in an enforcement action against Munchee Inc for its token offering, arguing that even if the tokens had a practical use when issued, they may still be securities. SEC Chairman Jay Clayton has publicly reaffirmed this stance on multiple occasions, stating that marketing coins as ‘utility tokens’ will not preclude them from SEC scrutiny.

Additionally, the SEC recently issued a statement warning exchanges that offer trading of digital assets that are deemed securities that they must register with the SEC as a national securities exchange or be exempt from registration requirements.

Under its 2013 guidance, the Treasury Department’s Financial Crimes Enforcement Network (FinCEN) stated that those in the business of exchanging and circulating virtual currencies are money services businesses subject to Bank Secrecy Act (BSA) regulation. An individual who obtains virtual currency to purchase goods or services, however, is not subject to money service business registration, reporting and recordkeeping requirements. FinCEN has issued two enforcement actions against virtual currency businesses for violating BSA requirements since publishing the guidance.

The Treasury Department’s Office of the Inspector General’s Annual Plan also highlights virtual currencies as a particular area of concern as a money laundering instrument, and notes that Treasury is examining how FinCEN identifies, prioritises and addresses money laundering and terrorism risks associated with virtual currency.

Additionally, there are currently two proposals relevant to combatting virtual currency use in money laundering schemes. One would establish an independent task force to combat terrorist and illicit use of virtual currencies, while the other would expand the definition of financial institution under the BSA to include issuers of digital currencies and require a report be submitted to Congress on a strategy infrastructure needed to detect digital currencies at border crossings.

The IRS declared through Notice 2014-21 that cryptocurrencies are to be treated as ‘property’ and not foreign currency for US tax purposes. As a result, any taxpayer who receives cryptocurrency in exchange for goods or services when computing gross income must report the fair market value of the cryptocurrency measured in US dollars at the time of the transaction. Notice 2014-21 also states that transactions involving cryptocurrency are taxable under the general tax principles applicable to property transactions and that cryptocurrency may be held as a capital asset in the hands of taxpayers. Despite industry calls for further clarification, the IRS has not provided any subsequent guidance.
The Tax Cuts and Jobs Act of 2017 limited the scope of 1031 tax-free like-kind exchanges under the Internal Revenue Code to real property. This likely means that when cryptocurrency is traded for like-kind property, the transaction may no longer receive 1031 treatment and may thus be taxable.

There is no legislation or regulation preventing tokens from being offered to US residents by international issuers. However, international issuers of tokens often choose to exclude US residents from participating in offerings due to potential regulation. If the token is deemed a commodity under US law, an international issuer may be subject to CFTC anti-fraud and anti-manipulation regulation, along with regulations on leveraged transactions. The SEC has also made it clear that some tokens may be classified as securities subject to US securities laws, meaning if an international issuer offers a token to a US resident and the token is considered a security, the international issuer will be forced to comply with US securities, tax and anti-money laundering regulations, among others.

Regulators have taken a cautious stance towards US residents’ participation in international token sales. While they have not provided any specific guidance on the matter, many have repeatedly warned market participants that regulators may be unable to obtain information from persons or entities located overseas, and that they may be unable to retrieve any lost or stolen funds.

VI OTHER NEW BUSINESS MODELS

Fintech business models are still developing, providing traditional financial services to consumers in more innovative, direct ways, and leveraging new technologies, including blockchain, for doing so. While fully automated financial services are not part of the model, and self-executing contracts and fully automated investment advisers a future possibility, fintech firms are particularly adept at using artificial intelligence and big data to make the borrowing and investing experience easier to execute online and more complete. In addition to licensing and regulatory issues that these activities raise, as discussed above, they also raise issues relating to data protection and data ownership that are only beginning to be addressed.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

Fintech endeavours may use a combination of patents, copyrights, trade secrets and trademarks to secure and protect their intellectual property rights.

Regarding patent protections, fintech companies’ inventions often involve methods practised using computer technology. As such, it is important to consider the patentability of such methods. While patent protection of methods at first may appear broad, recent court decisions have narrowed it considerably. In *Alice Corporation Pty. Ltd v. CLS Bank International*, the Supreme Court held that certain claims in a patent were ineligible for patent protection because they constituted an abstract idea. Under United States law, abstract ideas are not patentable. Furthermore, claiming the use of a generic computer implementation failed to transform the abstract idea into patent-eligible subject matter. Thus, under *Alice*, methods that simply require an otherwise abstract method to be performed on a computer will not be considered patent-eligible subject matter. It is important for fintech businesses to consider this restriction when evaluating how to protect their intellectual property. Their business models, as concepts, or proprietary operations carried out by software may not be eligible for patents.

© 2019 Law Business Research Ltd
In terms of copyright, software code and certain works within software applications, such as original visual design elements and original text are protected. Copyright prohibits others from making or distributing copies of a firm’s software without permission. Copyright does not prohibit others from independently developing similar software.

Finally, fintech companies can protect their inventions and innovations, particularly the source code in computer programs, through trade secret law. Unlike patents and copyright, trade secrets do not expire. Since trade secrets are primarily protected by state law, there is a patchwork of different laws protecting trade secrets across the United States. However, in 2016, the Defend Trade Secrets Act created a federal cause of action for trade secret misappropriation. Fintech companies should be aware that trade secrets must be continuously guarded by them from public disclosure and do not protect against independent development by another party.

Fintech companies may also use trademarks in order to prevent others from using their names or other signifiers, such as logos, or from using names or logos that are confusingly similar. Trademarks do not protect business models or proprietary technology, but they may be valuable in establishing and protecting a brand identity or positioning a firm within a market.

i Ownership of intellectual property
Ownership rights in inventions originate in the inventor. Whether the inventions are ultimately protected by patent or trade secret, the inventor is the initial owner of such intellectual property. Similarly, ownership in copyright originates with the author of the copyrighted work, unless the copyrighted work is a work made for hire, in which case, provided certain formalities are followed, the employer or entity that commissioned the work is considered its author for purposes of copyright ownership.

Every fintech company should take steps to make sure that it owns the intellectual property created by its employees or contractors, or otherwise generated by or for its business. To do so, a firm may insert an intellectual property assignment clause into all contracts with employees and contractors. Such a clause acts as an assignment of, and requires the employee or contractor to assign, all rights to the firm in any inventions, works or other intellectual property made during the engagement or in the course of employment. This clause may also specify that any copyrightable works made by the employee or contractor during the term of engagement are, by agreement of the parties, works made for hire with the authorship attributed to the firm. Similar provisions may be included in agreements with service providers.

Such agreements with employees and independent contractors may be drafted such that the salary or payment acts as consideration for the assignment of intellectual property. Under US law, no additional compensation must be paid to inventors or authors.

In addition, in order to protect trade secrets or other proprietary information of the firm, such contracts may contain confidentiality provisions that obligate the other party to maintain the confidentiality of all proprietary information received or generated by them in the course of employment or during the engagement.

ii Privacy and data protection
In the United States, there is no national data protection law, and no single or centralised authority is charged with jurisdiction over privacy and data protection issues. Rather, the
United States has taken a sectoral approach, with a variety applicable federal and state laws, and numerous federal and state agencies have authority to make and enforce rules in this area, depending on industry and context.

For fintech firms, applicable federal laws include the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), the Federal Trade Commission Act (FTC Act) and the Electronic Communications Privacy Act (ECPA). Obligations under such laws vary, from obligations to provide adequate notice of a firm’s data practices, to maintaining appropriate security measures for individuals’ financial information, to specific requirements for the use of consumer credit reports. The rules that may apply to a firm may depend on the nature of the firm and the type of data that it handles, and may be affected by other contextual factors. (Fintech firms that maintain an online presence should also be aware of the Children’s Online Privacy Protection Act, and those that interact with health data should be aware of their obligations under the Health Insurance Portability and Accountability Act.)

Similarly, numerous federal agencies have authority to enforce privacy and data protection rules, and agencies with applicable jurisdiction may vary by firm, based on the nature of the firm and the data it holds. Key federal agencies charged with responsibility in this area include the SEC, OCC, CFTC, CFPB and FTC. Most if not all of these regulators have stated that cybersecurity is a pressing and systemic concern deserving of investment and scrutiny. In addition, states’ attorneys general have authority to bring suits against firms in order to enforce state privacy and data protection laws.

**VIII YEAR IN REVIEW**

Over the past year, the US regulators, policymakers and courts have continued to focus on the issue of how virtual currency markets should be regulated and who should regulate them.

The CFTC chairman has touted the potential for technological innovations, including blockchain and digital ledger technology, to transform the way that regulators gather information and lower operational costs for financial institutions. The regulatory challenges stem from rapid technological developments, the disintermediation of key economic actors and the high levels of technological literacy necessary for regulators to keep pace. To address these issues, the CFTC has developed policies with the certain elements in mind, including adopting an exponential growth mindset that is predicated on anticipating market developments; creating an internal fintech stakeholder in LabCFTC; becoming a quantitative regulator capable of robust data collection, automated data analytics and artificial intelligence deployment; and embracing market-based solutions, rather than applying a ‘paternalistic hand on markets’ to steer them in regulators’ preferred direction. This reinforces the CFTC’s ‘do no harm’ approach to fintech regulation to date.

Meanwhile, the SEC chairman has reiterated the SEC’s ‘facts and circumstances’ position as to whether a digital asset transaction involves the offer and sale of a security and highlighted the agency’s balanced regulatory approach, which ‘fosters responsible innovation in this area, while also protecting investors and markets’. The SEC chairman has acknowledged market participants’ requests for further dialogue on the subject of when a token offering is a security, and has said that SEC staff are currently drafting additional guidance that will further assist market participants in determining whether a digital asset is offered or sold as a security.
IX  OUTLOOK AND CONCLUSIONS

As this area continues to develop, we expect to see further clarity regarding regulatory oversight over fintech-related matters.
ABOUT THE AUTHORS

STEPHEN ADAMS  
Collas Crill  
Stephen has been practising British Virgin Islands law for close to two decades, advising on a full range of corporate cross-border matters including joint ventures, mergers, acquisition finance, asset and project finance, investment funds, alternative investments, private equity and capital market transactions. 

He also has considerable experience in trust and private client matters, having held senior positions in several trust and corporate services businesses. 

Stephen joined the firm from Bedell Cristin where he headed up the firm’s BVI practice in Asia, having been instrumental in the launch of the Singapore office in 2012. Prior to that, Stephen founded BVI law firm Barker Adams following his role as corporate senior partner at Walkers in the BVI. 

Stephen is a member of STEP and the Singapore Institute of Directors. He also acts as non-executive director for a select number of prominent hedge funds.

ISABEL AGUILAR ALONSO  
Uría Menéndez  
Isabel Aguilar Alonso joined the firm in 2008 and is a counsel. 

She has more than 10 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.

JORDAN ALTMAN  
Shearman & Sterling  
Jordan Altman, a partner in the intellectual property transactions group and mergers and acquisitions group of Shearman & Sterling, practises corporate law with an emphasis on structuring, drafting and negotiating agreements that focus on the development, transfer, procurement, commercialisation and maintenance of intellectual property and technology.
Mr Altman also counsels clients on intellectual property portfolio development, including public companies, as well as growing technology-driven businesses and start-ups. He has extensive experience working with clients in the pharmaceutical, medical device, chemical, entertainment, sports, automotive, software and financial service sectors.

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 equity and debt crowdfunding platforms, P2P lending platforms, online lending intermediary based platforms, online money transfer systems, online payment system providers, robo-advisers, virtual stored value facility providers, 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* 2019. One source comments 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 2019: 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.

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.

© 2019 Law Business Research Ltd
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.

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 has been awarded with the Client Choice Award 2017 and 2018 for Banking in Belgium. He is also ranked as a leading individual by The Legal 500, and 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

Alexei has worked in the capital markets and banking and finance areas since 1996, developing broad expertise in fintechs and payment institutions, assisting companies with banking regulatory matters such as P2P loans, equity crowdfunding, payment service providers, bitcoin and blockchain technology, and asset management, among others.

Alexei is a member of the Financial Innovation Laboratory (created by the Inter-American Development Bank), the Brazilian Development Association and the Brazilian Securities and Exchange Commission. He is an officer at the capital markets forum of the International Bar Association, professor of investment funds in the master’s programme at GVlaw (Fundação Getulio Vargas) and professor of capital markets at ANBIMA (the Brazilian Financial and Capital Markets Association). He is certified as a compliance and ethics professional by the Society of Corporate Compliance and Ethics.

Alexei has an LLM in banking and finance from the London School of Economics and Political Science, and is a graduate of the Law School of PUC-SP (the Pontifical Catholic University of São Paulo).

SANDY BRUMBERG

Loyens & Loeff 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 & Partners
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 administration degree from a Dutch business school and a diploma from a US law school. 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 transactions. He also has experience in fintech and payment services matters, and blockchain/DLT, having worked in advising payment and e-money institutions as well as crowdfunding platforms.

CARLA DO COUTO HELLU BATTILANA
TozziniFreire Advogados
A partner in the information technology, data privacy and intellectual property practice, Carla has more than 10 years of experience assisting local and international clients in corporate and regulatory matters, and participating in several transactions, including mergers and acquisitions, joint ventures and corporate restructurings. Carla also focuses her work on assisting tech companies in corporate matters and transactions, as well as preparing and reviewing their terms of use and privacy policies.

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.
VICTOR CABRAL FONSECA
TozziniFreire Advogados

An innovation specialist and associate in TozziniFreire’s technology and innovation practice group, Victor is responsible for coordinating ThinkFuture, the first innovation programme structured by a full-service law firm in Brazil. As a lawyer, he assists technology-based clients, and major companies interested in open innovation and startups. He is a professor of law and startups at Insper (SP), holds a master’s degree in business law and economic and social development from FGV-SP and is certified in exponential innovation from Singularity University. Victor has published several articles about the subject and is also one of the authors of Direito das Startups, the first Brazilian book on the matter with full original content, published by Saraiva in 2018. He is pitch coach for Law Without Walls (University of Miami), a founding member of the Committee for the Studies of the Legislation on Creative Entrepreneurship and Startups of OAB/SP – Pinheiros, and cofounder of Legal Hackers – São Paulo chapter.

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 startup 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.

KONSTANTINOS GEORGIOU
Loyens & Loeff Luxembourg Sàrl
Konstantinos has been an associate in the banking and finance practice group since 2018. He specialises in banking and financing work including advising both borrowers and lenders on a broad range of national and cross-border finance transactions, secured lending and refinancing, with a particular focus on real estate finance, acquisition finance and fund finance.

BRYAN HOLLMANN
Stadler Völkel Rechtsanwälte GmbH
Bryan Hollmann is counsel at Stadler Völkel Rechtsanwälte GmbH, and is admitted as an attorney in New York. His practice focuses on the intersection of US law and cryptocurrencies, particularly with regard to securities, commodities and money transmitter laws in the United States. He frequently advises clients on the legal structure of ICOs, STOs, exempt securities offerings and concurrent US/EU offerings as well as anti-money laundering and customer due diligence matters. Before joining Stadler Völkel, Bryan served as a federal law clerk in the US District Court for the Northern District of Texas. He graduated from The George Washington University Law School in 2015 and obtained an LLM degree in corporate and securities law from the London School of Economics and Political Science in 2016.

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 HSIUNG

*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, startups, 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.

ROY KAMP

*McAfee*

Roy is McAfee's EMEA data protection officer. Prior to joining McAfee, he held legal roles in the services industry, including companies such as Michael Page. From the vantage point of the EMEA legal team, Roy is particularly interested in contracts and is a self-confessed privacy geek. He holds an LLB and LLM from University of Kent and CIPP/E credentials from the International Association of Privacy Professionals.

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 Malaysian 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.

**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. 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.

**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 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, his practice also focuses on assisting clients with the financial regulatory aspects of transactions in the fields of funds and M&A and capital markets.

MARIA EUGENIA GEVE DE MORAES LACERDA
TozziniFreire Advogados
Maria Eugenia Geve de Moraes Lacerda is an associate in the information technology, data privacy and intellectual property practice of TozziniFreire Advogados.

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 licencing 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.

STÉPHANIE LIEBAERT

*DLA Piper UK LLP*

Stéphanie Liebaert is an associate in the Antwerp office. She advises Belgian and foreign multinationals on all aspects of banking, financial services, funds and insurance law. Insurance regulatory, complex contracting assignments, privacy and IP issues in the financial industry, as well as fintech- and insurtech-related assignments, are her core areas of practice.

Stéphanie has a law degree from University of Antwerp. She studied abroad in France (Toulouse) and obtained a master of law degree (LLM) in IP and competition law from University of Liège.

THAÍS HELENA VALENTE TEIXEIRA LIMA

*TozziniFreire Advogados*

Thaís Helena Valente Teixeira Lima is an associate in the capital markets and banking and finance practice groups of TozziniFreire Advogados.

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.

LETTICIA 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.

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).

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.
IVAN ANTONIO MONTEIRO MARQUES
TozziniFreire Advogados
A senior associate of TozziniFreire Advogados, Ivan has over 12 years of experience in corporate law, especially with banking and financing projects, digital law and fintechs, capital market and M&A projects, having worked for major financial institutions and law firms. Ivan currently works with greenfield projects and makes deals for fintechs, with regulation and supervision from the Brazilian Central Bank. Moreover, he works with all tech ecosystems, including structuring investment funds to fintechs, partnerships with Brazilian financial institutions, formal solicitations to become a Brazilian financial institution and payment institutions at the Brazilian Central Bank.

TIAGO CORREIA MOREIRA
Vieira de Almeida
Tiago joined VdA in 2003. He is a managing associate 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 aviation finance transactions, having worked with export credit agencies and the main financing entities involved therein.

STEPHEN NELSON
Collas Crill
Steve is a partner practising in the investment funds and corporate and commercial departments. His practice is concentrated on investment funds and corporate finance. His clients include funds, investment managers, fund administrators, banks, family offices, financial houses and early stage companies.

Steve regularly advises investment managers on fund formation, registration with the Cayman Islands Monetary Authority, and listing on the Cayman Islands Stock Exchange. He also has extensive experience in the financing of early stage technology companies.

Prior to joining Collas Crill, Steve practised in Canada with Blake Cassels & Graydon, and before that in Kuwait with Al Sarraf & Al Ruwayeh (in association with Stephenson Harwood).

The 2019 Chambers and Partners Global Guide has designated Steve as an 'up and coming lawyer' for Cayman in the field of corporate and finance law.

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.
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.

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.

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).

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.
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 2019* ranks Peter in Band 1 for fintech.

ERIC ROTURIER
*Allen & Overy LLP*

Eric Roturier is a senior associate in Allen & Overy’s international capital markets department in Paris. He advises a wide range of financial services providers (including insurers) on the impact of both national and international regulatory regimes on their operations, on strategic corporate transactions involving regulated financial services entities and on the regulation of both retail and wholesale financial products and services. He also has wide-ranging experience with derivatives, structured finance and capital markets.

Before joining Allen & Overy LLP in 2010, he worked for two years in the financial services office at EY in Paris on tax issues. He graduated from ESSEC Business School (Paris and Singapore) with a major in finance, and obtained a master’s degree in business law and a master’s degree in philosophy from the University of Paris-Sorbonne.

Since 2017, he has been a member of Paris Europlace’s working group on blockchain and ICOs.

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.

REENA AGRAWAL SAHNI
Shearman & Sterling

Reena Agrawal Sahni is a partner in the global financial institutions advisory and financial regulatory practice at Shearman & Sterling. She focuses on US bank regulation, advising US and non-US banks and other financial institutions. Among other things, she advises on Dodd-Frank related regulations, including enhanced prudential standards, recovery and resolution planning, and the Volcker Rule. She also advises on financial institution M&A, capital markets transactions and financial institution insolvency issues. Reena also represents clients on corporate governance, OFAC and AML compliance, internal investigations and regulatory enforcement actions. Reena co-leads the firm's fintech initiative, working with payments companies and market infrastructure providers on a range of legal and regulatory issues.

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.

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 as ‘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.

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 purchases of shares and digital assets at the Katholieke Universiteit Leuven, Belgium (KU Leuven). He has published several articles on corporate law and blockchain, 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.

OLIVER VÖLKEL
Stadler Völkel Rechtsanwälte GmbH

Oliver Völkel is a founding partner of Stadler Völkel Rechtsanwälte GmbH, and is admitted as an attorney in Austria. Oliver advises companies in all stages of capital market issuings and private placements, both national and international. He advises on legal matters concerning cryptocurrencies, banking matters, regulatory matters, capital markets regulation, general corporate and corporate criminal matters. In particular, Oliver has experience in structuring new forms of financing such as initial coin offerings, initial token offerings and security token offerings. His clients include numerous well-known Austrian and foreign companies and banks. Oliver Völkel studied law at the University of Vienna, where he also worked as an assistant professor, and at the Columbia Law School in New York. In the past, he worked in the criminal law department at the University of Vienna, among others, as well as in renowned international law firms. He is a lecturer at the law faculty of the University of Vienna and an arbitrator of the Chamber of Commerce’s permanent arbitration court in Vienna.

NOÉMIE WEINBAUM
McAfee

With nearly 20 years of experience in information technology law and privacy, 10 of which were spent in the finance sector as the deputy head of legal shared services for Natixis, Noémie holds a long record in negotiating complex deals in international and regulated contexts, and in supporting business evolution and success. She also provides regulatory advice in the sphere of banking and payments, as well as in privacy, and more generally in the legal impacts of data management. Noémie holds an LLM and CIPP-E, and has been admitted to the Paris Bar since 2003. As an individual, she is committed to promoting innovation and the continued success of business by fostering balanced protection of IP rights, as well as legal and contractual trust in the use of technology and in the responsible, protected collection and processing of people’s data. Noémie regularly publishes articles and participates in debates on these issues.
ALEXANDER YAP WEI-MING

*Allen & Gledhill LLP*

Alexander is co-head of Allen & Gledhill’s fintech practice.

In the area of fintech, Alexander often advises on internet banking, online trading, electronic contracting, electronic document retention, cybersecurity, and various innovations in the delivery of financial and insurance services, including preparing related user and service agreements for Singapore or global roll-outs. A contact partner and specialist on Personal Data Protection Act 2012 (PDPA) issues, he regularly directs clients’ PDPA, data protection and privacy compliance activities, and advises on data breaches.

Alexander was named by *Global Data Review* as one of the world’s best upcoming generation of data lawyers under the age of 40, in their 40 Under 40 survey, and is one of only two South-East Asian lawyers in the list. He is recommended for his expertise in intellectual property work by *The Legal 500 Asia Pacific 2019* and is noted to be ‘a key name for commercial transactions relating to intellectual property, information technology and the protection and management of data’.

Alexander is recognised by *Who’s Who Legal* in its Banking 2019: Fintech Analysis as a leading individual in Asia Pacific. *Who’s Who Legal* also notes that 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 graduated from the University of Oxford with an MA in jurisprudence. He joined Allen & Gledhill in 2006 and was called to the Singapore Bar in the same year. He was also admitted as a non-practising solicitor of England and Wales.

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.
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

ALLEN & OVERY LLP
52 avenue Hoche
75008 Paris
France
Tel: +33 1 40 06 53 86
Fax: +33 1 40 06 54 54
eric.roturier@allenovery.com
www.allenovery.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: +44 117 307 6000
gareth.malna@burges-salmon.com
sarah.kenshall@burges-salmon.com
www.burges-salmon.com

BUZKO & PARTNERS
3–5 Bolshaya Morskaya Street, Suite 512
St Petersburg 191186
Russia
Tel: +7 812 924 05 88
roman.buzko@buzko.legal
www.buzko.legal

COLLAS CRILL
125 Main Street
PO Box 144
Road Town
Tortola
British Virgin Islands
Tel: +65 6800 4334
stephen.adams@collascrill.com
Floor 2, Willow House
Cricket Square
PO Box 709
Grand Cayman KY1-1107
Cayman Islands
Tel: +1 345 914 9606
stephen.nelson@collascrill.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

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
9F, 201 T‘un Hua N Road
Taipei 10508
Taiwan
Tel: +886 2 2183 2232 / +886 2 2183 2162
Fax: +886 2 2514 9841
abesung@leeandli.com
eddiehsiung@leeandli.com
www.leeandli.com

GILBERT + TOBIN
Lever 35, Tower Two
International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000
Australia
Tel: +61 2 9263 4000
Fax: +61 2 9263 4111
preeves@gtlaw.com.au
www.gtlaw.com.au

GLENEAGLES

© 2019 Law Business Research Ltd
LOYENS & LOEFF
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

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
konstantinos.georgiou@loyensloeff.com
sandy.brumberg@loyensloeff.com

www.loyensloeff.com

MCAFEE
McAfee Security UK Limited
6th Floor, The Urban Building
3–9 Albert Street
Slough SL1 2BE
United Kingdom
Tel: +44 845 528 0235
roy_kamp@mcafee.com

16th floor
11-13 Cours Valmy a La Defense
92800 Puteaux
France
Tel: +33 1 4762 5600
noemie_weinbaum@mcafee.com

www.mcafee.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@mhmjapan.com
takane.hori@mhmjapan.com
takahiro.iiijima@mhmjapan.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

NOERR LLP
Boersenstraße 1
60313 Frankfurt am Main
Germany
Tel: +49 69 971477252
Fax: +49 30 20942094
jens.kunz@noerr.com
www.noerr.com

SHEARMAN & STERLING
599 Lexington Avenue
New York
NY 10022
United States
Tel: +1 212 848 7125 / 7324
jordan.altman@shearman.com
reena.sahni@shearman.com
www.shearman.com

© 2019 Law Business Research Ltd
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

URÍA MENÉNDEZ
c/ Príncipe de Vergara, 187
Plaza de Rodrigo Uría
Madrid 28002
Spain
Tel: +34 91 586 03 72
Fax: +34 91 586 04 00
leticia.lopez-lapuente@uria.com
isabel.aguilar@uria.com
www.uria.com

STADLER VÖLKER
RECHTSANWÄLTE GMBH
Seilerstätte 24
1010 Vienna
Austria
Tel: +43 1 997 1025
Fax: +43 1 997 1025 99
oliver.voelkel@svlaw.at
bryan.hollmann@svlaw.at
www.svlaw.at

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
www.vda.pt

TOZZINIFREIRE ADVOGADOS
Rua Borges Lagoa 1328
São Paulo 04038-904
Brazil
Tel: +55 11 5086-5000
abonamim@tozzinifreire.com.br
ccouto@tozzinifreire.com.br
iamarques@tozzinifreire.com.br
melacerda@tozzinifreire.com.br
thlima@tozzinifreire.com.br
tfonseca@tozzinifreire.com.br
tozzinifreire.com.br