ACKNOWLEDGEMENTS

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

ALLEN & GLEDSHILL LLP
ALTENBURGER LTD LEGAL + TAX
ANAGNOSTOPOULOS
BDO LLP
BRUCHOU, FERNÁNDEZ MADERO & LOMBARDI
CEREBRA CPAS & ADVISORS
CMS VON ERLACH PONCET LTD
DEBEVOISE & PLIMPTON LLP
DE PEDRAZA ABOGADOS, SLP
GLOBAL LAW OFFICE
KOLCUOĞLU DEMİRKAN KOÇAKLI
LATHAM & WATKINS
LINKLATERS LLP
MATHESON
MOMO-O, MATSUO & NAMBA
MORAIS LEITÃO, GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS
NYMAN GIBSON MIRALIS
SETTERWALLS ADVOKATBYRÅ AB
SHARDUL AMARCHAND MANGALDAS & CO
SHIN & KIM
SIQUEIRA CASTRO ADVOGADOS
SLAUGHTER AND MAY
SOŁTYŚIŃSKI KAWECKI & SZLĘZAK
STUDIO LEGALE PULITANÒ-ZANCHETTI
SULLIVAN & CROMWELL LLP
WKK LAW RECHTSANWÄLTE
## CONTENTS

PREFACE.......................................................................................................................................................... vii  
*Nicolas Bourrin*

Chapter 1  
THE EVOLUTION OF THE ROLE OF THE FORENSIC ACCOUNTANT IN INTERNATIONAL INVESTIGATIONS ................................................................. 1  
*Stephen Peters & Natalie Butcher*

Chapter 2  
THE CHALLENGES OF MANAGING MULTI-JURISDICTIONAL CRIMINAL INVESTIGATIONS ........................................................................................................... 8  
*Frederick T Davis and Thomas Jenkins*

Chapter 3  
EU OVERVIEW ........................................................................................................................................ 23  
*Stefaan Loosveld and Sarah Benzidi*

Chapter 4  
ARGENTINA ........................................................................................................................................... 32  
*Fernando Felipe Basch, Guillermo Jorge and Gabriel Lozano*

Chapter 5  
AUSTRALIA ........................................................................................................................................... 43  
*Dennis Miralis, Phillip Gibson and Jasmina Ceic*

Chapter 6  
AUSTRIA ............................................................................................................................................... 58  
*Norbert Wess, Markus Machan and Vanessa McAllister*

Chapter 7  
BELGIUM ............................................................................................................................................... 68  
*Stefaan Loosveld and Sarah Benzidi*

Chapter 8  
BRAZIL ................................................................................................................................................... 82  
*João Daniel Rassi, Victor Labate and Pedro Luis de Almeida Camargo*

Chapter 9  
CHINA .................................................................................................................................................... 92  
*Alan Zhou and Jacky Li*
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Country</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>ENGLAND AND WALES</td>
<td>Stuart Alford QC, Mair Williams and Harriet Slater</td>
<td>102</td>
</tr>
<tr>
<td>11</td>
<td>FRANCE</td>
<td>Antoine Kirry, Frederick T Davis and Alexandre Bich</td>
<td>121</td>
</tr>
<tr>
<td>12</td>
<td>GREECE</td>
<td>Ilias G Anagnostopoulos and Jerina (Gerasimoula) Zapanti</td>
<td>136</td>
</tr>
<tr>
<td>13</td>
<td>HONG KONG</td>
<td>Wynne Mok and Kevin Warburton</td>
<td>144</td>
</tr>
<tr>
<td>14</td>
<td>INDIA</td>
<td>Anuj Berry, Nishant Joshi, Sourabh Rath and Kunal Singh</td>
<td>160</td>
</tr>
<tr>
<td>15</td>
<td>IRELAND</td>
<td>Karen Reynolds and Ciana Dunny</td>
<td>169</td>
</tr>
<tr>
<td>16</td>
<td>ITALY</td>
<td>Mario Zanchetti</td>
<td>189</td>
</tr>
<tr>
<td>17</td>
<td>JAPAN</td>
<td>Rin Moriguchi and Ryota Asakura</td>
<td>207</td>
</tr>
<tr>
<td>18</td>
<td>POLAND</td>
<td>Tomasz Konopka</td>
<td>217</td>
</tr>
<tr>
<td>19</td>
<td>PORTUGAL</td>
<td>João Matos Viana, João Lima Cluny and Tiago Coelho Magalhães</td>
<td>228</td>
</tr>
<tr>
<td>20</td>
<td>SINGAPORE</td>
<td>Jason Chan, Lee Bik Wei, Vincent Leow and Daren Shiau</td>
<td>242</td>
</tr>
<tr>
<td>21</td>
<td>SOUTH KOREA</td>
<td>Seong-Jin Choi, Tak-Kyun Hong and Kyle J Choi</td>
<td>256</td>
</tr>
<tr>
<td>22</td>
<td>SPAIN</td>
<td>Mar de Pedraza and Paula Martínez-Barros</td>
<td>266</td>
</tr>
<tr>
<td>23</td>
<td>SWEDEN</td>
<td>Ulf Djurberg and Ronja Kleiser</td>
<td>281</td>
</tr>
</tbody>
</table>
Contents

Chapter 24  SWITZERLAND ................................................................. 289
Bernhard Lötscher and Aline Wey Speirs

Chapter 25  TURKEY ................................................................. 304
Fikret Sebilcioğlu, Okan Demirkan and Begüm Biçer Ilikay

Chapter 26  UNITED STATES ............................................................ 313
Nicolas Bourtin and Steve A Hsieh

Appendix 1  ABOUT THE AUTHORS .................................................. 329

Appendix 2  CONTRIBUTORS’ CONTACT DETAILS .................................. 349
In the United States, it continues to be a rare day when newspaper headlines do not announce criminal or regulatory investigations or prosecutions of major financial institutions and other corporations. Foreign corruption. Healthcare, consumer and environmental fraud. Tax evasion. Price fixing. Manipulation of benchmark interest rates and foreign exchange trading. Export controls and other trade sanctions. US and non-US corporations alike have faced increasing scrutiny by US authorities for more than a decade, and their conduct, when deemed to run afoul of the law, continues to be punished severely by ever-increasing, record-breaking fines and the prosecution of corporate employees. And while in the past many corporate criminal investigations were resolved through deferred or non-prosecution agreements, the US Department of Justice has increasingly sought and obtained guilty pleas from corporate defendants. While the Trump administration has announced various policy modifications incrementally to moderate the US approach to resolving corporate investigations, the trend towards more enforcement and harsher penalties has continued.

This trend has by no means been limited to the United States; while the US government continues to lead the movement to globalise the prosecution of corporations, a number of non-US authorities appear determined to adopt the US model. Parallel corporate investigations in several countries increasingly compound the problems for companies, as conflicting statutes, regulations and rules of procedure and evidence make the path to compliance a treacherous one. What is more, government authorities forge their own prosecutorial alliances and share evidence, further complicating a company’s defence. These trends show no sign of abating.

As a result, corporate counsel around the world are increasingly called upon to advise their clients on the implications of criminal and regulatory investigations outside their own jurisdictions. This can be a daunting task, as the practice of criminal law – particularly corporate criminal law – is notorious for following unwritten rules and practices that cannot be gleaned from a simple review of a country’s criminal code. And while nothing can replace the considered advice of an expert local practitioner, a comprehensive review of the corporate investigation practices around the world will find a wide and grateful readership.

The authors who have contributed to this volume are acknowledged experts in the field of corporate investigations and leaders of the bars of their respective countries. We have attempted to distil their wisdom, experience and insight around the most common questions and concerns that corporate counsel face in guiding their clients through criminal or regulatory investigations. Under what circumstances can the corporate entity itself be charged with a crime? What are the possible penalties? Under what circumstances should a corporation voluntarily self-report potential misconduct on the part of its employees? Is it a realistic option for a corporation to defend itself at trial against a government agency? And
how does a corporation manage the delicate interactions with employees whose conduct is at issue? The International Investigations Review answers these questions and many more and will serve as an indispensable guide when your clients face criminal or regulatory scrutiny in a country other than your own. And while it will not qualify you to practise criminal law in a foreign country, it will highlight the major issues and critical characteristics of a given country’s legal system and will serve as an invaluable aid in engaging, advising and directing local counsel in that jurisdiction. We are proud that, in its tenth edition, this publication covers 25 jurisdictions.

This volume is the product of exceptional collaboration. I wish to commend and thank our publisher and all the contributors for their extraordinary gifts of time and thought. The subject matter is broad and the issues raised are deep, and a concise synthesis of a country’s legal framework and practice was challenging in each case.

Nicolas Bourtin
Sullivan & Cromwell LLP
New York
May 2020
Chapter 1

THE EVOLUTION OF THE ROLE OF THE FORENSIC ACCOUNTANT IN INTERNATIONAL INVESTIGATIONS

Stephen Peters & Natalie Butcher

I INTRODUCTION

It is now generally accepted that forensic accountants form an integral part of large-scale complex cross-border fraud investigations. This has not always been the case and raises the question as to whether forensic accountants are essential. In short, in the past the answer would have been no. In times gone by, fraud investigations would be undertaken by specialist investigators, many of whom were former enforcement officers. An accountant would be used specifically to look at the transactions in the books and records. A forensic accountant is not necessarily a specialised fraud investigator and, before forensic accounting became mainstream, fraud investigators managed without them.

However, the number and scale of international investigations has multiplied over the last few years and this has coincided with a significant increase in the range of skills and specialisms that the major forensic accounting teams now possess. Although the term ‘forensic accountant’ has a relatively narrow interpretation when it comes to the role of expert witness in litigation and arbitration matters, in terms of investigations it is now a generic description that extends its boundaries beyond accountants and accounting: it encompasses a diverse range of skills and expertise that is invaluable in complex investigations. This is not just traditional accounting analysis but also: (1) providing expert evidence in fraud bribery and corruption trials; (2) interviewing of witnesses; (3) imaging of devices; (4) data mining; (5) data interrogation; (6) data hosting; (7) provision of sector experts and industry knowledge; (8) asset tracing; (9) asset recovery; and (10) corporate intelligence. A forensic accounting practice typically offers forensic technology and e-disclosure services, large-scale document review capability, corporate intelligence skills and the ability to undertake general investigations. Furthermore, the size and diversity of offerings found in the larger accounting firms also allows an investigation team to bring in specific sector specialisms, utilising the powers of insolvency practitioners and valuation experts to support recovery efforts. Consequently, forensic accountants are commonly used by companies and their legal counsel to fulfil a wide range of investigative roles outside that of pure technical financial analysis.

This diversification in the role of the forensic accountant can be put down, in a large part, to two significant shifts in the business environment. Firstly, it is a response to globalisation, and the increasingly international nature of businesses, regulatory scrutiny and thus investigations. A large accounting firm will have professionals based in most countries of the world; it, therefore, will offer organisations and legal counsel the ability to deploy local resources quickly. It also reflects the fact that aspects of large international investigations

---

1 Stephen Peters is a partner and Natalie Butcher is a director at BDO LLP.
are heavily process-driven; as such, the skills and experience of legal counsel may be better focused on strategy and litigation. Secondly, the effect of digitisation means that the volume of data that needs to be collected and analysed has grown exponentially and it is forensic accounting teams that have invested heavily and now possess market leading expertise in this area.

Clearly, we are in an ever-changing world that has been highlighted in the most extreme of terms by the events of the first quarter of 2020. It will be some time before the full effects are known on the way that we interact and do business. What is certain is that new ways of working remotely, harnessing the power of technology, have come to the fore and these are likely to stay with us in one way or another. This will inevitably change the way in which investigations are carried out and, in turn, will undoubtedly lead to greater reliance on, and even faster growth in, the use of forensic technology. That said, it is likely that the fundamental principles underlying investigations will remain the same.

The role of the forensic accountant in international investigations in general follows a standard template: investigating the facts and circumstances underlying the issue through the analysis of financial records and interviews, supporting the document review and disclosure process, tracing the destination of any misappropriated funds or assets, and assisting with recovery efforts. Indeed the modern forensic accountant may be judged by the tools and techniques that can be brought to an investigation, rather than by the traditional core set of accountancy skills; understanding the techniques for extracting and analysing data or recovering assets in far-flung territories is as important now as an appreciation of the financial statements.

It goes without saying that the forensic accountant is not the only party involved in investigations. They form part of a wider multi-disciplinary team, both alongside specialists that are now deemed to fall under the ‘forensic accounting’ umbrella and together with management, in-house counsel, external lawyers and, on occasion, regulators.

II FINANCIAL ANALYSIS

As outlined above, the traditional role of the forensic accountant in investigations has been focused on the analysis of financial and accounting records. Although forensic accounting is now much broader than this, focused accounting analysis is still relevant. In general terms, any fraud, bribery or financial misconduct will be reflected in, and evidenced through, the financial and accounting records of an organisation. While a payment or transaction may be disguised or hidden, its existence will be recorded in the accounts, any absence producing an imbalance or reconciliation error and a pointer to an issue for the entity's management.

Thus, for example, the payment of bribes by an organisation may be recorded as, notionally, a legitimate expense: in the accounts payable ledger; as employee expenses or commissions; or as discounts in the accounts receivable ledger. The direct cost of procurement fraud may be disguised through the accounts payable ledger. Overly aggressive revenue recognition would be recorded in the accounts receivable ledger.

In the case of manipulation that is entirely ‘off the books’ as in the case of business diversion schemes where neither revenues nor any costs of sales are recognised in an organisation’s books and records, forensic analysis may be able to identify likely loss of profits from analysis of failed growth forecasts and other indicators such as falling market share.

Accounting treatments, and the individual technicalities of the underlying transactions can vary significantly between countries, industry sectors and size of organisations. Certain
industries have their own terminology, acronyms and jargon. It goes without saying that having the right mix of forensic accounting and sector-specific knowledge and experience in the investigation team is essential together with an appreciation of cultural differences; it may, for example, be desirable to include project accounting experience for an investigation at a construction company, or specific natural resources hedging expertise for a mining company.

Information gathering is a key component of a forensic accountant’s work and interviews form an important part of this. It would be very easy to undertake an analysis of accounting records that failed to progress an investigation if carried out blind. Hence, the accounting analysis benefits greatly from being informed and focused. The most effective accounting records analysis is performed with a full understanding of how the specific operations of the organisation in question relate to the underlying accounting records and suspected misconduct. The best way of achieving this is by interviewing. In general, although the interview process is more often than not conducted by legal counsel, in situations where a fraud or its concealment involves even moderately complex accounting manipulation or concealment, it is likely to be beneficial to include forensic accountants in the interviews.

### III ELECTRONIC DOCUMENT REVIEW AND E-DISCLOSURE

The world that we now live in is driven by technology and, as outlined in the introduction to this chapter, the events of 2020 have increased such reliance. It is difficult to imagine what our existence would be like without the digital revolution. Our computers, telephones and other mobile devices contain a digital fingerprint of our lives, both personal and business.

The volume of electronic data that we create on a daily basis has exploded and continues to grow exponentially. Ninety per cent of the world’s existing data has been created in the last two years: a single computer can hold several million documents; a typical mailbox will contain 50 to 100,000 emails. The volume of potentially relevant records of a global business involved in an international investigation may number hundreds of millions. In addition, the types of data being generated have drastically changed and become more complex. We now communicate in different ways through, for example, the use of Skype, WhatsApp and the like. These continual developments render the traditional methods of data capture, processing and analysis obsolete. We must also consider the evolving business and regulatory environments; business has become increasingly global, while there is a growing emphasis placed on data protection and cybersecurity.

In order to address these changes, new technology and methodologies are constantly being developed; this is an area that is moving rapidly. The most significant developments are outlined below but it may be that, because change is so rapid, they will already be out of date.

i Disclosure Pilot Scheme

As of 1 January 2019, a Disclosure Pilot Scheme has been in operation (with limited exceptions) in the Business and Property Courts of England and Wales. This aims to address the cost, scale and complexity of the disclosure process and encourage the use of new technologies to make the process more efficient and economical.

---

2 IBM’s Marketing Cloud.
Data collection and analysis

Data scoping is now an essential element of any data collection exercise; it is imperative that all sources of potentially relevant data are identified and located to plan an efficient and defensible strategy. A plethora of tools have been developed to capture and analyse the various types of data that are commonplace. These include audio-visual data, social media, instant messaging and workplace collaboration applications.

The prevalence of multinational companies that operate across country borders has driven an increased demand for a more cost-effective and efficient solution for the review of multilingual data. It is now the case that machine translation is a viable alternative to human translation. For the purpose of e-disclosure, this process can be fully integrated with the review platform to allow reviewers to seamlessly translate documents during the course of their work.

Cloud

Increasingly, companies are moving their corporate data to cloud-based systems to take advantage of cheaper storage. The e-disclosure industry is following suit; many of the largest e-discovery software providers now offer the option of a cloud-based solution, and many challengers are now entering the market with purely cloud-based offerings.

Artificial intelligence

Predictive coding has been touted as a miraculous solution to large and complex e-disclosure matters since the late 1990s. However, there has been a reluctance in the market to adopt this review strategy, particularly after a number of high-profile project failures resulting from poor planning or understanding. Since its judicial approval in the US in 2012, predictive coding has become a more accepted workflow, albeit in a measured capacity, because of more realistic expectations and a better understanding of its capabilities.

Further, the technology behind predictive coding has become more sophisticated; applications can now continuously learn from user input to constantly prioritise the most likely responsive data. This continual learning technology has had a quicker adoption than predictive coding, because of the simple implementation and more transparent workflow.

In addition to the above, many tools now offer investigators various options to analyse unstructured data without the use of keywords, such as through concept searching, sentiment analysis or the use of communication maps. These platforms allow the investigator to carry out simple early case assessment as well as discovering and exploring issues that may not have previously been identified.

Similar strides have been taken with regard to structured, typically financial, data. Platforms exist that automatically ingest significant volumes of transactional data from the most commonly used accounting systems and apply a number of tests to each, in order assign a risk score to every transaction. The system can also be trained on vast quantities of financial data to build an artificial intelligence model, thus negating the need for specific tests, but allowing anomalous transactions to be flagged automatically. The use of these technologies can identify the high-risk transactions within millions of records in minutes, and more effectively than the human eye. For example, anomalous flows of funds can be identified, which would be near-impossible for a human to detect.
The Evolution of the Role of the Forensic Accountant in International Investigations

IV ASSET TRACING

The challenges faced when attempting to trace assets are numerous: today’s sophisticated fraudster is able to move assets quickly, making use of the mobility of assets and funds offered by globalisation, by channelling and directing them through different jurisdictions and by changing their form. Cash can be moved effortlessly, through multiple jurisdictions and converted into non-cash assets, often being split and divided and channelled in different directions. We are commonly dealing with financially astute fraudsters who are able to take action to move and hide their stolen proceeds and take steps to frustrate recovery attempts by the legitimate owners. We are now also encountering the challenges of tracing when faced with cryptocurrencies, the fraudster seeing the attractions of the market’s pseudo-anonymity, decentralised nature, and loose regulation and exploiting this to launder the proceeds of the crime. While, with traditional money, fraudsters employ complicated and often sophisticated techniques involving shell companies, offshore bank accounts (sometimes temporary in nature), use of nominees, gatekeepers and other such intermediaries, in the case of cryptocurrencies, they may use various anonymisation techniques in attempts to obscure the money trail. On the face of it, this makes the potential for tracing impossible. However, one of the defining features of a cryptocurrency is that its ledger, which contains all transactions that have ever taken place, is globally visible. Interestingly, research has demonstrated that it is often possible to track flows of money as it changes hands, and in some cases to de-anonymise users entirely, even in cryptocurrencies that are specifically designed to achieve anonymity. This is an extremely important factor in relation to the tracing of funds being moved through the non-conventional financial system.

Whatever method is used by the fraudster to move the assets, victims and their legal advisers must embark upon an often lengthy and complex process of asset tracing to determine the location of the assets and to link identified assets to the crime and the offender. Every asset-tracing exercise has its unique complexities, but inevitably includes a more or less iterative process of gathering and analysing evidence of asset movement.

Tracing is an almost entirely linear process: following an asset as it is moved or substituted for another and, thereafter, another and so on. While assets may be split and recombined, and mixed with other funds, the tracing exercise moves in an essentially chronological progression. In a conventional asset tracing exercise, banking records in particular are the bread and butter, representing an accurate and reliable source of evidence. Indeed, it is often the case that the only record of a flow of assets will be held by the financial institution facilitating the transaction.

Even once the flow of assets has been established, there are further hurdles that need to be negotiated. Before steps can be taken to secure and freeze identified assets, by applying legal remedies such as search and third-party disclosure orders to obtain further evidence of asset movement, the rules of tracing need to be considered. The tracing exercise is merely a process by which a claimant demonstrates what has happened to his or her property, identifies its proceeds and the persons who have handled or received them, and justifies his or her claim that the proceeds can properly be regarded as representing his or her property.3 In English law, for example, there are separate rules in common law and equity that determine whether or not an asset is traceable.

3 Foskett v. McKeown [2001].
Common law tracing relies on the claimant having legal ownership of the property. It will fail if the property has been mixed with other property or the legal title has been transferred to anyone other than the victim. Where specific assets identified by common law tracing can be identified, a claimant will be entitled to claim them as his or her property. However, the major obstacle in respect of common law tracing is that assets cannot be traced once mixed with other funds. Tracing is, however, allowed through ‘clean substitutions’, meaning that if misappropriated funds are directly used to purchase another asset, ownership can be traced to and claimed in that substitute asset.

Due to the limits with common law tracing, equitable tracing is more commonly encountered in practice. It relies on there being an equitable interest in the property and can succeed where there has been mixing. Given that it is likely that the proceeds of a misappropriation will be transferred into a bank account containing funds belonging to others, the equitable remedy is important for victims of fraud.

Notwithstanding the above, the English courts in particular have demonstrated flexibility in application of the tracing rules. As such, this is an area where it is likely that the forensic accountant will work closely with counsel, with a clear division establishing itself: the forensic accountant focusing on the messy and complex business of analysing financial, corporate and banking records to follow the money; legal counsel considering the appropriate rules to apply.

V ASSET RECOVERY

Tracing the assets, however, is only the start. Arguably the most important aspect is recovery; in this regard the value of the assets is crucial – this must be weighed up against the costs of physical recovery and realisation where appropriate. The value of any underlying asset is often surrounded by uncertainty, particularly in cases where funds have been secured from third parties based upon spurious asset values: these assets consist of properties, businesses, shareholdings or entities that can be located in far-flung countries; consequently, they can prove to be extremely difficult to value. Once again, the sophisticated forensic accountant will be able to turn to specialists in his or her team who will be experienced in undertaking valuations of these assets with their associated complications.

In the case of both conventional assets and those of a more unusual nature, it needs to be established that it makes sense economically to pursue recovery. Once this appears to be the case, the method of doing so should be determined. There are a number of approaches that can be used to recover assets: the most usual route is by way of conventional litigation, albeit that this is often complicated by the need to litigate in a number of countries and different legal systems. The role of the forensic accountant then shifts to providing litigation support, feeding into various particulars of claim and witness statements, etc.

A less common, albeit potentially effective, route is to use the formal powers of insolvency practitioners to take control and ultimately realise the assets. Most insolvency practitioners in the UK are accountants or insolvency experts working in firms of accountants. Upon formal appointment, an insolvency practitioner takes on certain powers and responsibilities that can prove particularly helpful in gaining control of assets that would otherwise require an unwieldy and ultimately costly legal process to achieve the same end result. It is helpful that many of the offshore jurisdictions where control of such assets ultimately rests adopt the English legal system or variations thereof. The insolvency practitioner, once appointed, is
able to utilise his or her powers, often across borders, to control assets and ultimately realise them for the benefit of creditors (which, where there is fraud or misappropriation of assets, will likely include the victim).

In respect of insolvent entities, potential recoverable assets could be unconventional in their nature. For example, there may be outstanding litigation against certain parties or, indeed, claims that arise as a consequence of the insolvency itself. This may include such matters as professional negligence claims against advisers. This would likely involve the skills and expertise of a forensic accountant, this time not from a pure investigative capacity but as an adviser on quantum. The forensic accountant would协助 the insolvency practitioner (and his or her legal advisers) in quantifying the losses suffered and assisting with formulating the damages claim. The forensic accountant or (with independence in mind) another forensic accountant may ultimately be required to act as an expert under Civil Procedure Rule No. 35 or its equivalent in overseas jurisdictions should the matter proceed to litigation.
I INTRODUCTION

As the various chapters in this book demonstrate, managing a criminal investigation in one country is often a challenge in itself. This becomes much more complicated if prosecutors in more than one country are, or may become, involved. The applicable procedures and important protections, such as professional privileges, vary considerably from one country to another; perhaps more urgently, a strategy that may seem to be common sense or even obvious in one country may be ineffective or even counter-productive in another. This risk is not just theoretical; many crimes, such as corruption, money laundering, cybercrime and terrorism often cross borders. Evidence relating to the crime may be found in more than one country, and the prosecutors in more than one country may investigate and prosecute.

These situations are intrinsically complex and do not lend themselves to a one-size-fits-all approach. As this book shows, procedures differ enormously among countries and many are changing at a rapid pace, requiring frequent updates. Local knowledge and contacts are critical; weaving together a comprehensive multinational strategy will often depend on personal relationships with officials in the various countries.

That said, many traps for the unprepared can be anticipated. The goal of this chapter is not to offer a strategy for any particular case – that would be impossible – but rather to provide a basic checklist to address multi-jurisdictional risks. Even this checklist must be viewed as flexible. Among other things, while listed below in a logical sequence, it does not follow that one topic can be fully addressed before another is considered: they are often interactive, and urgent time exigencies may quickly disrupt a well-constructed plan.

II IDENTIFYING THE CLIENT

The identity of the client may appear obvious, but identifying the client precisely – clearly specifying the client’s goals and agreeing on a protocol, which is generally a good approach in any event – is particularly important in transnational cases because differing rules in the countries involved may pose threats to the confidentiality of attorney–client communications.

Representing corporate entities, for example, may present unique issues. A lawyer engaged to advise or represent a corporation may also need to interface with its parent or subsidiaries; in particular, if the corporation creates subsidiaries for tax or regulatory purposes,
the various entities may be under different disclosure and other regulatory obligations in their countries of incorporation. Once an investigation begins, they may be subject to different restraints, such as local secrecy, privacy or ‘blocking statute’ obligations (see Section IV.iii).

In some instances, the client may not be a corporation but an entity such as an audit committee that may act with some degree of independence. A company’s board of directors may establish a special ‘litigation committee’ or other group tasked with protecting shareholders’ interests. In these cases, the client’s goal may not be to develop a legal defence for the corporation but rather to satisfy audit, fiduciary and other obligations.

Joint ventures pose further problems. The extent of any one company’s responsibility for the acts of the joint venture, as well as control of its decision-making during an investigation, may be complex and depend upon differing local laws. In other cases, the client may be a person or entity such as an outside auditor whose interests may be to some degree aligned, but not identical, with a corporate target. A company’s responsibility to its officers and employees (such as an obligation to pay attorneys’ fees) may be governed by by-laws and vary considerably under local laws.

Once a corporate client is identified, it is imperative to specify the individuals within the corporate structure who will be the exclusive contacts with attorneys advising and representing it, and to establish a protocol governing those communications. While US procedures for maintaining attorney–client privilege are generally broad and flexible, other countries limit protected communications to those between outside lawyers (often limited to members of a local bar) and senior officials of the company capable of receiving and acting upon legal advice. Because communications between an attorney and anyone not so identified may not be protected and become the subject of compelled, non-consensual production to a prosecutor, an early task is to identify qualified individuals who can speak for the corporation and to establish a strict protocol limiting confidential communications to that group.2

Advising or representing a corporation generally precludes the ability to give legal advice to individuals associated with it, even senior officers such as the chief executive officer, an issue revisited in Section IV.iii regarding the Upjohn principles. Because a corporation and its officers may develop inconsistent or even hostile interests – if, for example, a corporate investigation reveals evidence incriminating an individual that the corporation may be pressured to share with prosecutors – clarifying and memorialising this distinction is important.

If the client is an individual, then, of course, there will be no difficulty in identifying him or her. But especially in complex corporate and multinational investigations, the lawyer must reach a specific retention agreement. Such an agreement may address the extent of the corporation’s agreement or obligation to pay the client’s fees (on which local laws may differ). In some instances, the lawyer may wish to consider a common defence agreement or other arrangement with corporate counsel or counsel for other individuals, but local law

---

2 The issue of the identity of the client within a corporate organisation was explored under UK law in Serious Fraud Office v. ENRC. The High Court decision (see The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Ltd [2017] EWHC 1017 (QB)) restricting protection, particularly where the corporate client could not demonstrate that it was anticipating adversarial litigation, was largely overturned on appeal, but Justice Andrews’ discussion of the need for a specified corporate contact to maintain confidentiality would appear to remain largely intact (see Serious Fraud Office v. Eurasian Natural Resources Corporation Ltd [2018] EWCA Civ 2006).
and professional practice may bear on the feasibility and safety of doing this. In others, the attorney may conclude that the client’s interests are unaligned with, or even hostile to, those of a corporate entity being investigated, and may need to take steps to protect the client’s interests during the investigation. The best strategy for doing so may vary country by country, depending, among other things, on local professional practice rules.

III IDENTIFYING THE COUNTRIES THAT MAY BECOME INVOLVED

The list of countries that may ultimately become involved in a criminal investigation will often change and must be constantly updated. It is, however, important to have a preliminary list before expending significant resources on fact-gathering, and certainly before developing a comprehensive long-term strategy.

Different national regimes may apply to two separate questions: First, which countries’ laws apply (or may apply) to the potentially criminal conduct at stake and to what degree may prosecutors in those countries become involved; and, second, what countries’ laws may apply to the evidence that may be related to the investigation. In many situations, the countries so implicated may be the same, but that is not always the case, and in any event, the relevant risks and questions are quite different.

i Laws applicable to conduct

Before committing resources to investigating facts, and certainly before providing a client with anything other than very short-term advice, it is imperative to determine which prosecutors are already involved, as well as those that may become so on their own initiative or that may need to be contacted. For each of them, it is important to have a preliminary but practical sense of each country’s laws and procedures relevant to the conduct in question. This book provides some indications of these differences across jurisdictions, but ultimately it is critical to get high-quality, savvy legal advice from a lawyer qualified and familiar with the laws and practices of each potentially involved country (and to do so under procedures that maximise professional protection of communications with such lawyers under applicable local rules). Among national variables are the following.

Substantive criminal laws

There has been some degree of convergence among the substantive criminal laws relating to financial and other corporate crimes in the countries covered in this volume. But this is not universally true. For example, even signatories to the Organisation for Economic Co-operation and Development’s Convention on Combating Bribery of Foreign Public Officials in International Business Transactions differ on how to define bribery, such as whether a ‘facilitating payment’ is permitted, and whether anti-corruption laws apply to passive bribery (bribe-takers) as well as active bribery (bribe-givers).  3


4 Under the FCPA, only the payment of a bribe (i.e., active bribery) is prohibited. However, under Section 2 of the UK’s Bribery Act, the receiving of a bribe is also criminalised. Similarly, there is a divergence between the United States and United Kingdom on the payment of ‘facilitating payments’. While the FCPA contains an express exception to permit such payments, under the Bribery Act they are not distinguished from other bribes.
Corporate criminal responsibility
National criminal laws differ widely on whether and under what circumstances corporate entities can be held criminally responsible (that is, convicted of a crime): some provide for no corporate criminal responsibility at all;5 some (such as the United States) provide for virtually automatic criminal responsibility under the principle of respondeat superior; some (such as the United Kingdom) provide for limited corporate criminal responsibility in some circumstances6 and much broader exposure in others;7 and others (e.g., France) have principles for corporate criminal responsibility that are somewhat vague and still being developed.8 The laws on this core issue will have a major impact on determining defensive corporate strategy, generally because corporations will be more vulnerable – and in many cases have a greater motivation to negotiate – in countries that do not provide legal arguments against corporate conviction.9

Time periods
Statutes of limitation vary significantly country by country. Variables include not only duration but also important factors such as fixing a ‘starting date’; whether or how it can be suspended (or ‘tolled’); and the circumstances under which it can be satisfied (whether by a formal investigation or the filing of a secret indictment, for example). They also vary as to whether and how they can be waived, which may become relevant during an investigation. In theory, an analysis could lead to a conclusion of diminished risk in a country with a short

5 This is the case in Germany, although the expansive use of administrative regulation of corporate misbehaviour may diminish its significance. See Edward B Diskant, ‘Comparative Corporate Criminal Responsibility: Exploring the Uniquely American Doctrine Through Comparative Criminal Procedure’, 118 Yale L. J. 2 (2008). See also the Korea chapter of this guide, which notes that ‘the Criminal Act, which traditionally covers most common types of crimes, does not recognise corporate criminal liability,’ but that ‘various other statutes imposing industry-specific or subject-specific regulations (e.g., those on securities, construction, pharmaceuticals, public procurement, taxation, labour, competition, environment) usually recognise corporate criminal liability’.

6 Under the ‘identification principle’ in the United Kingdom, corporations can be convicted of a crime only if the ‘directing mind’ – generally board members or very senior officers – were aware of acts committed by employees and approved them. See Pinto & Evans, Corporate Criminal Responsibility (2008).

7 Section 7 of the UK Bribery Act of 2010 created a new ‘corporate offence’ by which corporate entities can be held virtually strictly liable if its ‘associated persons’ commit certain kinds of bribery or other offences for the benefit of the corporation, and the corporation had not adopted procedures that could reasonably have been expected to deter such conduct. The UK Bribery Act of 2010: A Guide to the New Offences, www.debevoise.com/insights/publications/2010/05/the-uk-bribery-act-2010-a-guide-to-the-new-offen__.

8 Article 121-2 of the French Penal Code provides that corporate entities (other than the state) can be held liable for acts committed ‘on its account’ by ‘organs or representatives’ of the entity. The French courts have not been entirely clear how to interpret the requirement that the offending individual be a ‘representative’ of the corporation, an issue that has led to corporate acquittals notwithstanding felonious acts by an employee. Davis, ‘Limited Corporate Criminal Liability Impedes French Enforcement of Foreign Bribery Laws’, https://globallanticorruptionblog.com/2016/09/01/guest-post-unduly-limited-corporate-criminal-liability-impedes-french-enforcement-of-foreign-bribery-laws/.

9 Recognising the importance of this issue, the Organization for Economic Cooperation & Development (OECD) set up a working group to explore differences in national regimes and published a comprehensive report in December 2016: www.oecd.org/corporate/liability-of-legal-persons-for-foreign-bribery-sto cktaking-report.htm.

© 2020 Law Business Research Ltd
The Challenges of Managing Multi-jurisdictional Criminal Investigations

The Challenges of Managing Multi-jurisdictional Criminal Investigations

The challenges of managing multi-jurisdictional criminal investigations are significant, as the laws and legal systems of different countries can vary widely. One of the primary challenges is the statute of limitation, although it should be emphasised that anticipatory analyses of statutory periods can be risky because the laws are often complex, and facts yet undiscovered can affect the analysis.

**The availability of advantageous outcomes through self-reporting**

The passage of time may have another, less obvious impact on country-by-country prioritisation: some countries offer complete leniency, or at least hugely advantageous outcomes, to cooperating corporations – but only to companies that genuinely ‘self-report’ by bringing matters to the attention of prosecutors before prosecutors discover the conduct on their own, or in some instances by self-reporting before a competitor does. The cost of losing such an opportunity by being ‘too late’ may be significant, so it is often extremely important to understand if one may be available, but is subject to being lost, in key countries under consideration.

**Territorial and double jeopardy limits**

The territorial limits on a prosecutor’s power (including whether the laws of that country apply to the conduct in question) and the ability of authorities in one country to prosecute a person or company that has already been convicted or acquitted in another country have traditionally not been determinative issues with respect to US investigations. Unlike in many European countries, American criminal laws rarely formalise their territorial limitations, so that territorial limits are generally decided by judges case by case and in generally it is often difficult in the United States to obtain a judicial ruling on territorial constraints in a criminal prosecution prior to trial. Perhaps, as a result, US prosecutors often proceed on an assumption that they are authorised to investigate any potential crime that has any connection at all with the United States, such as the use of US dollars. Separately, American law systematically does not recognise a criminal outcome from a different ‘sovereign’ as triggering any rights under the double-jeopardy clause of the Constitution. Further, American law generally permits both a prosecutor (such as the Department of Justice) and a regulator (such as the Securities and Exchange Commission) to seek and obtain penalties relating to the same defendant and the same facts, even though the ‘sovereign’ is the same.

This latitude may not be the case in other countries, particularly in Europe, where recent trends suggest limits on multiple and extraterritorial prosecutions. Continental European and other code-based countries often specify the territorial conditions under which its criminal laws apply. Under some circumstances that may vary by jurisdiction, the domestic laws of some countries may oblige its prosecutors not to prosecute individuals or companies already convicted or acquitted elsewhere, which may come as a surprise to American lawyers. Regional treaties may apply double jeopardy (or ne bis in idem) principles across national boundaries. Regional bodies such as Eurojust (located in The Hague) may allocate prosecutorial responsibility to one country or another, to avoid a free-for-all of

---


multiple prosecutions. There are also indications that the principle that no person should be twice tried for the same facts or offence may come to be viewed as a human right recognised by supranational principles based on human rights.

European laws may also provide advantages not available in the United States with regard to parallel criminal and regulatory investigations. While the issue is complicated and subject to evolution, the European Court of Human Rights, as well as some national courts, have recognised the unfairness of permitting a double recovery by criminal prosecutors and regulators in the same country, in essence forcing the authorities of that country to choose one or the other.

The law relating to territoriality may be evolving in the United States. Following the decision of the US Supreme Court in *Morrison v. National Australian Bank,* that court and others have become more vigilant in assessing whether the application of US laws – and the power of a US prosecutor to enforce them – is justified in any particular case. This has led to a debate over the proper territorial reach of US prosecutions and in one instance the dismissal of key charges brought under the Foreign Corrupt Practices Act for lack of a territorial connection. This trend may, over time, make the United States a less potent threat to corporations incorporated and active only outside the United States, although as noted (see footnote 10) raising territorial challenges in United States courts is procedurally challenging. The applicability of the relevant principles is very fact-intensive and can only be developed on the basis of the mastery of the relevant facts.

### ii Laws applicable to evidence

Getting access to, obtaining or copying, and often transmitting across national borders potential evidence – including information obtained by interview – often runs into local law issues that can bedevil an investigation if not planned properly. Differing laws and practices, for example, may apply depending upon the physical location of documents (or physical things) and the physical location of a person whose information is sought by an interview (and, occasionally, the citizenship of that person).

Among the possible constraints are privacy and database issues. A company seeking to learn about its own employees’ conduct, for example, must be wary of creating legal issues in gaining access to those employees’ emails or records, particularly since the promulgation of the EU General Data Protection Regulation (GDPR) in 2018. The issue becomes more

---

15 See Davis, op. cit. footnote 12.
18 *United States v. Hoskins,* 902 F.3d 69 (2d Cir. 2018).
complex when information stored as data is accessible from multiple countries, often from places different from its actual storage.\textsuperscript{20} Some countries’ regimes prohibit transferring certain kinds of personal data out of the country, which may be necessary during a transnational fact-gathering exercise.\textsuperscript{21}

Further, many countries have bank regulations governing access to, and dissemination of, customer banking information.\textsuperscript{22} Blocking statutes may also prohibit the transfer of any significant information out of the country in which it is stored. Most blocking statutes apply to transnational responses to state inquiries – by prohibiting response to a foreign subpoena, for example, unless the subpoena issuer proceeds through a bilateral or multilateral treaty. Such local statutes may apply, however, if a company expatriates information with the intent to share it with a foreign prosecutor or investigator.\textsuperscript{23}

Finally, local professional responsibility rules may restrict how interviews are done by lawyers.\textsuperscript{24}

\section*{iii Criminal procedures, practical culture and prioritisation by risk}

Most fundamentally, of course, one must develop a map of the countries that may become involved, and begin the process of prioritising them by risk and opportunities. To some degree, a review of criminal procedures (and, especially, potential criminal penalties, which may vary wildly) will provide guidance. But ultimately, every country has its own track record and culture with respect to transnational criminal matters, in which some have been notably more aggressive – and often more successful – than others. Some countries also offer much greater, or more advantageous, possibilities of reaching a negotiated outcome, and it is important to understand the state of the laws, procedures, and practices in different countries on this important issue.

Until relatively recently, a cynical but generally useful principle was a simple one: if in any given situation prosecutors in the United States were likely to become involved, that was by far the biggest threat; an ultimate strategy would focus on dealing with US prosecutors – often by negotiation. This strategy proceeded on the assumption (often correct) that US prosecutors would second-guess outcomes in other countries anyway, so that it generally made more sense to deal primarily with them in the belief that other countries’ authorities

\begin{footnotesize}
\begin{enumerate}
\item See Kirry, Davis & Bisch, ‘France’ in \textit{The International Investigations Review} (2020).
\item For example, the role of such protections in criminal investigations was explored in the pathbreaking agreement of the United States Department of Justice with Swiss banking giant UBS in 2009. See www.justice.gov/opa/pr/ubs-enters-deferred-prosecution-agreement.
\item The several different effects that differing professional rules may have on cross-border investigations are explored in Davis, ‘How national and local professional rules can mess up an international criminal investigation', https://globalinvestigationsreview.com/article/1194073/how-national-and-local-professional-rules-can-mess-up-an-international-criminal-investigation (17 June 2019).
\end{enumerate}
\end{footnotesize}
The Challenges of Managing Multi-jurisdictional Criminal Investigations

would fall into line with any outcome obtained in the United States. The rise of some significant outcomes in criminal investigations in Europe, however, may be changing that assumption, and an evaluation of risks and opportunities remains complex.

IV ESTABLISHING THE FACTS

A lawyer cannot professionally and competently advise a client on defensive strategy in a criminal investigation without understanding the relevant facts. A skillful, thorough and timely investment of effort to master an understanding of those facts can be a major factor in the success of developing an optimal strategy. This is particularly true if that strategy involves any form of negotiation with a prosecutor: counsel armed with a superior appreciation of the facts than an adversary will inevitably be better prepared to negotiate well for a client; counsel provided with an incomplete or, worse, misleading understanding of the facts will inevitably cede control to better-informed prosecutors and risk an irredeemable loss of credibility.

The crucial process of learning facts may be conceptualised as an internal investigation, and that phrase will be used here. The term ‘internal investigation’ has recently become freighted with connotations derived from the fact that such investigations have become a virtual cottage industry for members of the legal profession, and the existence or fruits of many investigations have become known to the public after they have been shared with prosecuting authorities in the course of negotiations. But it is important to emphasise that the process of learning facts through such an investigation – a crucial step in any representation – does not in any way include or suggest an obligation to share it with anyone other than a client.

What are the goals of an investigation?

What we think of as an ‘internal investigation’ may actually encompass several different tasks, with different goals and often different applicable rules. To avoid misunderstanding, there must be careful consideration given to an investigation’s goals so that appropriate procedures and protections apply to it.

At its simplest, any lawyer asked to advise or represent a client in a criminal matter will at an early stage ask a simple and obvious question: what happened? This enquiry often begins with questioning a client (if the client is an individual) or with discussions with an appropriate officer (if the client is a corporation). Such a straightforward act of fact-finding is a form of an internal investigation, and while questioning an individual client is generally simple enough, the process becomes much more complex when the client is a corporation, especially one with far-flung activities. By conducting a factual enquiry, the lawyer is, of course, fulfilling a professional obligation of diligence to learn the relevant facts to best advise the client on a defensive strategy. It may later emerge that the strategy will involve some form of negotiation, possibly on the basis of the factual investigation and sometimes sharing the results of that investigation with a prosecutor. However, in many cases, it is impossible to make a decision to communicate or negotiate with a prosecutor, or to share information,


27 Various different kinds of ‘internal investigations’ and their attributes are discussed in Davis, American Criminal Justice: An Introduction (2019), chapter 17.
without first learning the relevant facts sufficiently well to advise the client on that strategy, and permit the client to make an informed strategic choice. That process should take place only under procedures that guarantee confidentiality of the information learned as well as the advice given on the basis of it. Further, in a multinational investigation, it is imperative to understand the potentially different rules that may be applicable in different jurisdictions.28

In a relatively small subset of cases, a company may make a public declaration of the fact that it is conducting an investigation and a commitment that a report of it will be made public. This occasionally occurs when well-known companies are viewed as having been tainted by one form or another of criminal acts by one or more of its officers or employees; such an investigation is part of a public relations campaign to protect the company’s reputation. It is sometimes said that such an investigation is ‘independent’, meaning that its goal is to determine ‘what happened’ on a neutral basis, rather than to develop the best defence for a client;29 the reports of such ‘independent investigations’ are often designed to, and do, become public.30 In these unusual circumstances, protecting the confidentiality of the work product is not a core concern, as the work product may be designed for publication anyway rather than for defence in a criminal proceeding.

In most cases, however, an internal investigation begins as the attorneys’ professional effort to ascertain the relevant facts to advise and defend a client against possible or threatened prosecution. That advice may in fact later turn out to be to reach out to, and negotiate with, a prosecutor, and in some cases even to use the results of the attorney’s investigation in those communications. National variants on the extent to which doing so is protected by a professional or other privilege, and the steps necessary to ensure such confidentiality, that bear on timing, and that affect the use of investigations are discussed below. The critical point at the opening of an engagement is that thought be given to confirming with the client that the investigation is, in fact, subject to confidentiality protections, and to develop procedures to shield that confidentiality in the countries that may be involved.

ii What national rules may apply to lawyer-conducted investigations?

American lawyers benefit from traditions giving them ample professional authority to take steps to advise and represent their clients, and from professional protections – notably the attorney–client and work-product privileges – to shield their efforts from compelled production to a prosecutor. If properly set up and appropriately maintained, an internal investigation conducted in the United States will almost certainly be considered covered by one or both of these principles, and a demand by a prosecutor for the work product of an attorney – even if it is very likely that the ultimate purpose of the attorney’s efforts will be to share information with a prosecutor – will be rebuffed.31 Further, it is considered improper for a prosecutor to put pressure on a defendant, including a corporation, to waive its attorney–client privilege.32 This is true even if the lawyer conducting the inquiry is an

in-house counsel seeking information from fellow employees of the corporation.33 These protections cannot be taken for granted, however, in a multinational investigation, where the following variants may appear.

**Who qualifies as a ‘lawyer’?**

As noted, for many purposes – including the ability to conduct an internal investigation with appropriate professional protections – a duly qualified lawyer employed by a corporation to do legal work (such as a general counsel or a lawyer working in the general counsel’s office) qualifies in the United States as an ‘attorney’ for purposes of creating an attorney–client privilege and a work-product privilege. That is not the case in most European and many other countries where an in-house counsel cannot be, or remain, a member of the bar, from which it follows that communications between such a person and others within the corporation may not be protected.34

**What are the local practice-of-law requirements?**

Companies conducting a worldwide investigation often use one law firm to lead that effort, and it often happens that lawyers from that firm conduct, or at least participate in, evidence gathering and interviews in countries where they are not licensed to practise law. While tolerated in many instances, this practice is increasingly dangerous because local bars are clearly focused on the professional constraints affecting internal investigations and are not likely to look kindly on lawyers over whom they have no oversight who conduct such activities in their jurisdiction.35

**Can a lawyer conduct an internal investigation?**

In the United States, it goes without saying that attorneys can conduct internal investigations on behalf of their clients, and virtually all such investigations done in the United States are conducted, or at least supervised, by attorneys. This is not automatically true in other countries. In France, for example, it was popularly understood by many that a French lawyer should not be involved in an internal investigation, and few were. However, in 2016, almost certainly in response to a desire to regain market share from Americans and lawyers from other countries, the Paris Bar issued an opinion, later developed in several guidelines, providing that French attorneys can in fact conduct such investigations, and that they are subject to the French near-equivalent of the attorney–client privilege, emphasising that in doing so attorneys must be respectful of the rights of those they may interview.36 Prosecutors in some other countries have sometimes been able to seize materials relating to internal investigations from attorneys’ offices.37

---

34 The European Court of Justice so held with respect to competition cases before it in the often-cited decision of *Akso Nobel Chemicals v. Commission*, Judgment of 14 September 2010.
35 See Davis, op. cit., footnote 24.
36 See Kirry, Davis & Bisch, op. cit., footnote 21.
Do conditions support the application of a professional privilege?
In the United States, virtually any communication between an attorney and a client seeking legal advice (other than advice about how to commit a future crime, which may fall within the ‘crime fraud exception’ to the attorney–client privilege) will be protected from compelled disclosure. The professional laws in other countries, however, may be much more exigent with respect to the conditions necessary to support the assertion of a professional privilege. The High Court decision in *ENRC v. SFO* in 2016 seemed to hold that certain aspects of an investigation conducted by an attorney (particularly witness interviews) are protected by a professional privilege only after it is clear that an adversarial relationship exists with a prosecutor – that is, after a prosecutor has made a decision to prosecute. To the great relief of the defence bar in the United Kingdom and elsewhere, this holding was significantly revised on appeal, in a judgment that provided that as long as a company has some good-faith basis to believe that it is, or may be, the subject of a criminal investigation, its communications with attorneys – if appropriately conducted – will be protected against compelled production.38 The laws on this specific point may well vary by jurisdiction, and must be understood in detail with respect to any investigation done in any particular country.39

Can the work product of an internal investigation be used in negotiation?
It is often the case in the United States that an investigation that commenced as an entirely confidential matter shielded by the attorney–client (and possibly work-product) privilege then leads to negotiation discussions with a prosecutor. In such discussions, if the properly informed client specifically consents, the attorney may share with a prosecutor factual information learned during the investigation, even though it had previously been zealously protected from compelled production. The attorney may even physically transmit a written internal investigation report to be used as a basis for discussion, and in some circumstances that report may end up providing the ‘factual basis’ for a negotiated outcome such as a deferred prosecution agreement, a non-prosecution agreement or a guilty plea.

Conceptually, there is no professional impediment to doing so: in the United States, the attorney–client and work-product privileges are viewed as ‘belonging to’ the client, from which it follows that the client can, and expressly must before any communications with a prosecutor takes place, waive the applicable privilege, and thereby authorise the attorney to share otherwise privileged material. Professional obligations applicable to lawyers in other countries, however, may not work in the same way. In France, for example, it is said that even a client cannot ‘waive’ the French near-equivalent of the attorney–client privilege that prohibits an attorney from sharing information learned as a result of a professional engagement. Care must therefore be taken to make sure that the fruits of an internal investigation are used under procedures that respect the professional obligations of the lawyers who conducted it.

iii What are best practices for investigations in different countries?
Conducting a large corporate investigation in one country is daunting enough: each one must be carefully thought through to establish a practical plan that is effective, efficient, compliant with local norms and rules, and designed to provide useful and usable work product. The

---
39 See Davis, op. cit., footnote 37.
operational logistics can be difficult. Developing a work plan when the investigation spans more than one country adds significantly to this challenge. Among the issues that must be anticipated and addressed are the following.

**Developing a compliant data and document access and copying programme**

As already noted, the arrival of the GDPR in Europe and similar laws protecting privacy elsewhere creates a thicket of potential regulatory limits on information gathering. Such rules are generally local to the place where the data or other information are found, and the laws applicable to them must be understood and addressed.

**Logistics of database management and transfer**

A large investigation will inevitably result in compilation of large amounts of information that will be reduced to a form of digitised data. Local laws may impact the ability to maintain such databases, and also on rights to transfer data in them outside of the country.

**Possible coordination with prosecutors**

In many situations, counsel conducting an investigation may make a determination whether to reach out to a prosecutor relatively early in an investigation, possibly at its outset. There are often reasons why such an early contact can be advantageous. In some circumstances, local law may provide that the ‘first’ company to ‘self report’ its involvement in a crime, for example, may benefit from protection against prosecution, and even absent such specific provisions it is often advantageous to get the ear of a prosecutor before a whistle-blower or a competitor does so. Counsel can sometimes advantageously work out with a prosecutor the limits of an investigation. In particularly sensitive situations, the prosecutor may engage in what the US Department of Justice calls ‘deconfliction’, whereby the Department may direct a corporate investigator not to interview certain witnesses until after the prosecutor has had an opportunity to do so.40

In the context of mergers, the Department of Justice has issued guidelines offering to hold an acquiring company harmless for the pre-acquisition criminal acts committed by an acquired company if the acquiring company conducts a comprehensive post-acquisition investigation and shares its results with the prosecutor.41 In those situations, the prosecutor may want to exercise supervision and control of the investigation, even if conducted by corporate counsel.

The extent of prosecutorial involvement in an investigation may, however, lead to unforeseen consequences, particularly for the prosecutor. If a prosecutor gets heavily involved in supervising or controlling a purportedly ‘private’ investigation, in the United States a court may conclude that the private counsel’s acts are ‘fairly attributable to the government’ and thus subject to procedural restraints normally applicable to government investigators. This may include limits on the ability to ‘compel’ testimony without violating the interviewee’s

---


© 2020 Law Business Research Ltd
The Challenges of Managing Multi-jurisdictional Criminal Investigations

right to be protected against compelled self-incrimination, and may subject transfer of
the fruits of an interview out of a country to the restraints of ‘blocking statutes’ normally
applicable only to providing information to state actors.42

Upjohn warnings in interviews
The Supreme Court’s decision in Upjohn Co v. United States43 confirmed that an investigation
conducted in the United States by an attorney, including an in-house attorney, is covered by
the attorney–client privilege and the work-product privilege. It emphasised that, in the case
of a corporate investigation, the ‘client’ is the corporation and not a person being interviewed
during the investigation. From this, there developed the salutary practice of giving ‘Upjohn
warnings’ to employees of a corporate client who are formally interviewed, in which it is
emphasised that the attorney interviewing them is not advising or representing them, but
the corporation. From which it follows that the corporation may elect to use the fruits of the
interview without consulting the interviewee.

Interviews can lead to difficult situations that must be anticipated. What are an
attorney’s professional (and moral) obligations if it appears that an interviewee may make
self-incriminating statements? How does an attorney respond if an interviewee asks if he or
she should have separate counsel? Will the company pay for such counsel? Can an interviewee
demand to see a copy of notes? There is no simple answer to such questions; the most
appropriate response depends on sensitivity to the context, but also on local laws including
professional responsibility rules as well as the company’s by-laws and internal policies.

Other local variants
Local customs and practices, as well as laws, may affect the conduct of interviews. Workers’
councils in many countries will take an interest in any systematic programme of interviewing
employees and will want to be consulted. If a company is conducting an investigation as
part of a programme of ‘cooperation’ with a prosecutor, the prospect of information being so
shared may well create internal labour difficulties.

V DEVISING A COMPREHENSIVE STRATEGY
The most important step is also the most complicated and the least amenable to a checklist:
developing a coherent and effective defence in the face of multiple investigations. A few
principles may guide the process.

There must first be a short-term strategy.44 Following the steps outlined here may well
take time, during which events may progress. External events generally cannot be controlled,
but at least some events internal to the client may be subject to review and modification. Chief
among them is the risk that relevant evidence will become unavailable or even destroyed,
which can have devastating results in an investigation, especially if prosecutors conclude that
the destruction was wilful or should have been avoided. In most circumstances, it is imperative

42 See Davis, op. cit., footnote 23.
insights/publications/2019/01/beginning-an-internal-investigation.
to issue ‘hold notices’ to relevant employees directing them not to destroy documents or other evidence, even in the course of a routine clean-up. Local laws and practices may inform how this is done to conform with workplace and other norms.

A strategy must be flexible, and constantly reviewed and updated. The steps outlined here may well suggest a strategy that turns out to be suboptimal when new facts emerge, or perhaps when new actors (such as prosecutors in new countries) become involved.

Consequential decisions must be based on a maximum of available inputs. While time pressures may put pressure on prompt decision-making, it nonetheless is imperative to accomplish as much as possible of the checklist found here before important decisions are made. Reaching out to a prosecutor, for example, is a weighty step because, once done, it will inevitably set in motion reactions that can be anticipated but not controlled. A coherent strategy will evaluate the range of possible outcomes from any proposed step. If not performed with the facts known and a sophisticated understanding of the various actors who may become involved, this strategy is unlikely to achieve its goals.

Performing an internal investigation does not always lead to negotiations with a prosecutor or a decision to reach out to one, but a possible decision to self-report must be at least considered in most cases. Especially in the United States, relatively few corporations actually proceed to a criminal trial; in most cases, a negotiated process can predictably reach an outcome preferable to a predicted trial outcome, largely because it is relatively easy in the United States to convict corporate entities, for reasons summarised in Section III.i. The Department of Justice is increasingly clear that it not only expects corporations to self-report, but that if good faith promptness and cooperation are demonstrated, the corporation will be well rewarded, often by avoiding a criminal conviction that could have otherwise have disastrous consequences. As a result, other countries are increasingly exploring negotiated outcomes often similar to those long available in the United States. The procedures and practices relating to whether, how and when to reach out to a prosecutor, and most importantly the degree to which one can negotiate with a prosecutor, vary tremendously by country, as this book demonstrates. Hiring experienced local counsel is critical; relying on instincts from one’s own country may often lead to suboptimal outcomes, even a disaster.

The consequences of a negotiated outcome must be explored with the client. Guilty pleas may result in being barred from public or other contracts under local, national or regional rules. Even a successful negotiation – one that leads to a ‘declination’ or a non-criminal outcome, such as a deferred prosecution agreement – may have consequences that need to be analysed through the perspective of the different countries that may be affected. The appointment of a monitor, for example, may create local legal issues, including whether a local blocking statute permits the monitor to report to officials in another country. More generally, an obligation of ‘cooperation’ whereby a corporation delivers evidence incriminating its officers or its employees may raise local issues, including under workplace rules.

45 In March 2019, Swiss banking giant UBS and its French subsidiary were convicted in French court of money laundering and other crimes related to alleged tax evasion by their clients, and were hit with fines and other payments totaling almost €4 billion, having rejected a negotiated outcome that would have resulted in a far smaller result. While the judgment is being reviewed on appeal, its size and the apparent availability to obtain a much better outcome through negotiation may suggest a shift in strategy relating to companies subject to prosecution in France. See ‘French Criminal Court Imposes Blockbuster Fine for Tax Fraud Related Offences’ www.debevoise.com/insights/publications/2019/02/ french-criminal-court-imposes.
If the facts of a case cross borders, one cannot rely on the luxury of having to deal with a single national prosecutor, because communication and possible coordination among prosecutors must be anticipated and explored. Perhaps the most difficult issue may be deciding which prosecutor to approach (if, of course, any contact is made at all), and whether to also inform prosecutors in other countries at the same time, possibly on a coordinated basis. The problem is that in the general absence of a double-jeopardy (or *ne bis in idem*) protection across state borders, an outcome in one country may not preclude a new investigation in other – and the risk of a ‘me too’ prosecution. In very limited circumstances, *ne bis in idem* rules in fact may offer some protection, but in most instances, the best approach is to evaluate which country’s authorities are most likely to reach a result that will be both optimal to the corporate client and acceptable to prosecutors in other countries that could become involved. As noted in Section III.iii, traditionally this has led to a practical conclusion that it is safest to deal with American prosecutors if there is a real possibility of their involvement, as a US outcome stands a good chance of being accepted elsewhere (often because the penalties are so very high), while the opposite is often not true. This may be changing. In many instances, a company should evaluate the range of possibilities that could predictably follow a self-report in its ‘home’ country and determine whether an outcome there would be respected by other countries, including the United States. While couched in very vague terms (and specifically identified as ‘non-binding’ in a legal sense), the Department of Justice regularly issues guidelines emphasising that it does not wish to relitigate outcomes in other countries and will respect them – as long as they are ‘adequate’.46 A sophisticated understanding of the laws, procedures and especially the practices in the various countries that are or may be involved should lead to a reasoned judgement as to how to prioritise outreach to and communications among them.

Chapter 3

EU OVERVIEW

Stefaan Loosveld and Sarah Benzidi

I  INTRODUCTION

Criminal law in the European Union is an area that still falls within the remit of each Member State. Hence, the rules on whether or not a corporate can be criminally liable and on the criminal sanctions in the event of liability vary according to the relevant Member State, including in areas that concern the transposition of EU Directives (for instance on financial services and banking) that require Member States to establish sanctions.

Having said that, there is a variety of EU authorities and regulators that, albeit strictly speaking active in the regulatory and administrative field, have far-reaching investigative and sanctioning powers as well. These powers often do not differ significantly from those of criminal authorities. Because of the nature and effects of the measures taken and sanctions imposed by regulators on the corporates and individuals (e.g., senior management) affected by them, these persons often benefit from the same fundamental rights and guarantees under EU and national law that apply to purely criminal sanctions.2

Well-known examples of such regulatory authorities are the EU competition authorities (which wield powers across all sectors and areas of economic activity) and the EU financial and banking regulators (which supervise, investigate and sanction the conduct and activities of financial services providers, including banks). Other authorities, while created pursuant to Member States’ national law, find their investigation and enforcement powers in EU regulations. This is, for example, the case for national data protection authorities that investigate and enforce potential breaches of the General Data Protection Regulation (GDPR).3

II  CONDUCT

i  EU competition law: the example of leniency

Undertakings are not obliged to self-report when they discover an internal wrongdoing that could constitute a competition law infringement. They may, however, voluntarily opt to do so in competition cases to benefit from a leniency programme.

1 Stefaan Loosveld is a partner and Sarah Benzidi is an associate at Linklaters LLP.
2 The possible application of the criminal aspects of Article 6 of the European Convention on Human Rights is based on the criteria laid down by the European Court of Human Rights in Engel and others v. the Netherlands, 8 June 1976, 5100/71, paragraphs 82–83.
Under EU competition law, the conditions and benefits of leniency applications are enumerated in the Commission Notice on immunity from fines and reduction of fines in cartel cases (Commission Leniency Notice).\(^4\) Undertakings that are part of a cartel can apply for leniency. By contrast, abuses of dominant position, vertical agreements and horizontal agreements that are not cartels within the meaning of the Commission Leniency Notice cannot benefit from the leniency programme.

Leniency is granted on a first-come, first-served basis. If an undertaking or association of undertakings wants to obtain full immunity from fines, it must be the first to submit information and evidence enabling the European Commission to carry out a targeted inspection or to establish an infringement. A company that does not qualify for full immunity can apply for a reduction of the fine if it provides evidence that represents significant added value to the evidence already in the possession of the European Commission. In all cases, the leniency applicant must also end its involvement in the alleged cartel (except when the European Commission decides otherwise to preserve the integrity of the inspections), cooperate fully and expeditiously with the European Commission throughout its investigation, and provide all evidence in its possession. The applicant may not destroy, falsify or conceal any evidence relating to the alleged cartel, either prior to the submission of the application or during the investigation.

In assessing whether the conditions for leniency are satisfied, the European Commission enjoys a margin of discretion.

A company cannot be certain whether the competition authorities will consider the information provided to be sufficient to qualify for immunity or fine reduction. Also, leniency applications, under European competition law, provide no protection against private law claims for damages from customers or competitors.

Under the Antitrust Damages Directive,\(^5\) final decisions by the competition authorities constitute irrefutable proof of fault in private damage claims. The Antitrust Damages Directive also facilitates disclosure of evidence. However, leniency statements are shielded from requests for disclosure. Other documents in the investigation file may be disclosed, albeit that the court must balance the interests of the victims with the interest of effective public enforcement of competition law (i.e., keeping the leniency programme attractive for undertakings).

### ii EU financial services and banking: the example of whistle-blowing

As further shown below, various EU legislations in the area of banking and financial services or dealing with a specific topic (e.g., anti-money laundering (AML)) already contain a number of obligations to set up whistle-blowing mechanisms.

---

\(^4\) Commission Notice on immunity from fines and reduction of fines in cartel cases (OJ C 298, 8 December 2006, p. 17).


Until recently, there was no cross-sectoral EU legislation dealing with such mechanisms generally. This has changed with the adoption on 7 October 2019 of the Whistle-blowing Directive (the Directive). EU Member States have until 17 December 2021 to implement the Directive into their national legislation.

This Directive lays down minimum standards for the protection of ‘reporting persons’ (i.e., individuals (natural persons) reporting or publicly disclosing information on breaches acquired in the context of their work-related activities) and ‘persons concerned’ (i.e., individuals or legal entities who are referred to in the report or public disclosure as persons to whom the breach is attributed or with which they are associated). The employment status of the reporting person, and whether or not that person works in the private or public sector, is irrelevant. The protection also applies to, for instance, shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including the non-executive members thereof.

The breaches relate to an extensive list of EU legislations in a variety of areas that go beyond financial services or AML. They also include, among others, public procurement, product safety, transport safety, protection of the environment, food safety and health, consumer protection, the protection of privacy and personal data, and IT-security. This Directive contains in this sense the ‘default rules’, whereas the rules on whistle-blowing that are contained in specific EU legislation will continue to apply.

The Directive first obliges EU Member States to ensure that legal entities set up internal reporting channels and procedures. As a rule, this obligation does not apply to legal entities in the private sector with fewer than 50 employees. As an exception, undertakings that are active in the financial sector or that are otherwise obliged entities for AML purposes are always captured by this obligation. Legal entities in the private sector with 50 to 249 employees are allowed to share resources for the receipt and possibly investigation of whistle-blowing reports.

EU Member States are also obliged to establish external reporting channels and to designate to this effect the authorities competent to receive, give feedback and follow up on reports. As the Directive captures more areas than those for which there are currently already competent authorities in place for such external reporting, EU Member States will undoubtedly need to establish new authorities that are specifically competent for such reporting.

Besides internal and external reporting channels, the Directive also protects in certain circumstances ‘public disclosures’ (i.e., persons who publicly disclose information on breaches falling within the scope of the directive).

Finally, the Directive obliges EU Member States to provide for a wide range of protections for reporting persons and persons concerned. These cover, among others, the confidentiality of their identity (albeit with important exceptions), the compliant processing of their personal data and the protection against retaliation.

---


7 The Directive provides for the possibility for EU Members to grant similar exemptions for legal entities in the public sector.
EU Overview

**EU whistle-blowing legislation in the area of financial services**

At the EU level, various pieces of legislation in the areas of financial services generally and banking specifically also contain rules on the establishment of whistle-blowing mechanisms. These mechanisms also typically have an internal dimension (i.e., procedures for the reporting by employees to their employer of possible infringements) and an external dimension (i.e., procedures with the regulators for the reporting by employees or other persons that deal with financial services firms or banks of possible infringements to the regulators).

Thus, for instance, Article 32 of the EU Market Abuse Regulation\(^8\) requires Member States to ensure that the respective national administrative authority that is competent for market abuse infringements establishes effective mechanisms to enable reporting of actual or potential infringements of this Regulation. These mechanisms must include at least:

\(a\) specific procedures for the receipt of reports of infringements and their follow-up, including the establishment of secure communication channels for such reports;

\(b\) within their employment, appropriate protection for persons working under a contract of employment, who report infringements or are accused of infringements, against retaliation, discrimination or other types of unfair treatment at a minimum; and

\(c\) protection of personal data both of the person who reports the infringement and the natural person who allegedly committed the infringement, including protection in relation to preserving the confidentiality of their identity, at all stages of the procedure without prejudice to disclosure of information being required by national law in the context of investigations or subsequent judicial proceedings.

In the same context, the Market Abuse Regulation also obliges Member States to require employers who carry out regulated activities to have in place appropriate internal procedures for their employees to report infringements of the Regulation.

Finally, the Market Abuse Regulation allows Member States to provide for financial incentives to persons who offer relevant information about potential infringements of the Regulation to be granted in accordance with national law where those persons do not have other pre-existing legal or contractual duties to report the information. The conditions for the provision of these incentives are that (1) the information is new, and (2) it results in the imposition of an administrative or criminal sanction, or the taking of another administrative measure, for an infringement of the Regulation.

---

A similar requirement to establish internal and external whistle-blowing mechanisms is also provided for in other EU legislation, such as, for instance, in relation to MiFID II, undertakings for collective investment in transferable securities (UCITS), insurance distribution and packaged retail and insurance-based investment products (PRIIPs).

Finally, the same requirement exists in relation to the activities and supervision of credit institutions. The details of this requirement are laid down in Article 71 of the 2013 EU Banking Directive. The whistle-blowing mechanism to be established thereunder is to encourage the reporting of potential or actual breaches of both the national provisions implementing the 2013 EU Banking Directive and the 2013 EU Banking Regulation.

As regards credit institutions in the eurozone, the European Central Bank (ECB) obviously has an essential supervisory role to play, being at the helm of the Single Supervisory Mechanism (SSM). As the competent authority within the meaning of the aforementioned Article 71, the ECB has set up a ‘breach-reporting mechanism’. The rules and procedures governing this mechanism are laid down in Articles 36 to 38 of the SSM Framework Regulation. They set forth that any person may, in good faith, submit a report directly to the ECB if that person has reasonable grounds for believing that the report will show breaches of the ‘relevant EU law’ by the institutions supervised by the ECB or by the supervisors themselves (both the ECB and the national competent authorities for banking supervision). Where a breach relates to other areas of activity by a bank that do not fall under the ECB’s supervisory competences (e.g., consumer protection or the implementation...
of anti-money laundering rules), it is outside the ECB’s mandate to follow up on the breach. Instead, the breach should be reported to the national authorities that are competent for these areas. All personal data concerning both the person who does the reporting and the person who is allegedly responsible for the breach shall be protected in compliance with the EU data protection framework. Also, the ECB shall not reveal the identity of a person who has made such a report without first obtaining that person’s explicit consent, unless disclosure is required by a court order in the context of further investigations or subsequent judicial proceedings.

With regard to significant supervised entities, that is, those entities that are directly supervised by the ECB, the ECB itself assesses the report. By contrast, with regard to less significant supervised entities, the ECB only assesses reports for breaches of ECB regulations or decisions. The ECB forwards reports concerning less significant supervised entities to the relevant national competent authority, without communicating the identity of the person who made the report, unless that person provides his or her explicit consent.

While anyone who has knowledge of a potential breach may report this to the ECB, the ECB has indicated that compliance officers, auditors and other employees of a bank are the groups that are more likely to have knowledge of possible wrongdoing. The breaches that are most commonly reported to the ECB concern the inadequate calculation of own funds and capital requirements as well as governance issues within credit institutions.

iii Investigation of potential breaches of data protection legislation

Since 25 May 2018, the GDPR governs the processing (i.e., any sort of operation, including the mere storage) of personal data (wholly or partly) by automated means and the processing of personal data that forms part of a filing system (even if it is not processed by automated means) within the European Union.\(^\text{17}\) The person (individuals or legal entities) processing personal data and determining the purposes and the means of a processing is defined as the ‘controller’. The identifiable individual to whom personal data relates is defined as the ‘data subject’. The GDPR also defines a third category of actors that are qualified as ‘processors’ (i.e., persons processing personal data under the instructions of a controller).

In addition to setting out the general legal regime for such processing activities, the GDPR contains provisions in relation to investigations of potential breaches and their enforcement. It requires Member States to provide for at least one public authority to be in charge of the monitoring of the application of its provisions. It also sets out requirements in relation to the independence of the authority and qualification of its members, as well as their tasks and powers.

Among these tasks, national supervisory authorities are required to (1) monitor and enforce the application of the GDPR, (2) handle complaints lodged by a data subject (i.e., the individual to whom the personal data relates), or by a body, organisation or association and to investigate the subject-matter and keep the complainant informed of such investigation, (3) conduct investigations, including on the basis of information received by another authority.

---

17 In certain cases, the GDPR also applies to processing of personal data outside of the EU. See Article 3 of the GDPR as well as Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, European Data Protection Board, 13 November 2019.
In conducting their tasks, the national supervisory authorities must be granted the following investigative powers:

- ordering controllers or processors to provide any information they require for the performance of their tasks;
- carrying out data protection audits;
- reviewing data protection certifications;
- notifying a controller or processor of an alleged infringement of the GDPR; and
- obtaining access to all personal data and to all information necessary for the performance of their tasks and access to any premises, including to any data processing equipment and means, in accordance with EU or national procedural law.

In practice, many investigations by national supervisory authorities are launched following a notification of a 'personal data breach' (i.e., a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed). Under the GDPR, controllers are required to notify personal data breaches to the competent national supervisory authority without undue delay, and at the latest, within 72 hours of becoming aware of such data protection breach, unless it is unlikely to result in a risk to the rights and freedom of natural persons.\(^{18}\)

### III ENFORCEMENT

#### i EU competition law

Under EU competition law, the European Commission may impose fines on corporates of up to 10 per cent of the annual consolidated worldwide turnover of the undertaking. In setting the fine, the European Commission takes into account the gravity and duration of the infringement. The Fining Guidelines provide more guidance on how the European Commission will exactly calculate the fines.\(^{19}\) These Guidelines are not binding on the European courts, which exercise full jurisdiction and can review the fine. However, the instances when the European courts have adjusted fines in competition cases remain exceptional. A 10 per cent reduction of the fine can be granted under EU competition law if an undertaking agrees to enter into a settlement with the competition authority. In doing so, the undertaking concerned must admit its involvement in the infringement.

#### ii EU financial services and banking

The SSM started in November 2014 and is one of the four pillars of the EU Banking Union. It is particularly relevant for the supervision of credit institutions in the eurozone. It is composed of the ECB and the national authorities that are competent for the supervision of credit institutions in their respective EU Member State. The ECB has a key role in the SSM, as it is responsible for its effective and consistent functioning. In addition, it has, among the thousands of credit institutions that are established in the eurozone, full and direct supervisory

---

\(^{18}\) In certain cases, a personal data breach must also be communicated to the data subjects (see Article 34 of the GDPR).

\(^{19}\) Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No. 1/2003 (OJ C 210, 1 September 2006, p. 2).
authority over ‘significant institutions’. To ensure compliance with the supervisory rules and its regulations and decisions in this area, the ECB has significant supervisory, investigatory and sanctioning powers.

The ECB’s investigatory powers are similar to those that have been granted to other EU financial supervisory authorities, such as the European Securities and Markets Authority in the areas of supervision of over-the-counter derivatives, central counterparties and trade repositories, and of credit rating agencies. Thus, the ECB has the right to require legal and natural persons to provide all information that is necessary to carry out its supervisory tasks. It also has the right to require the submission and examination of documents, books and records, to obtain written or oral explanations from the representatives or staff of such persons, and to conduct all necessary on-site inspections at the business premises of the institutions under its supervision, including without prior announcement.

If an institution supervised by the ECB, intentionally or negligently, breaches a requirement under directly applicable EU law for which administrative sanctions are made available, then the ECB has the right to start a sanctioning procedure and impose administrative pecuniary sanctions. The same right exists in case of breaches of regulations or decisions adopted by the ECB in exercising its supervisory tasks. The ECB also has the right to publish the imposition of such sanctions, irrespective of whether or not a decision has been appealed. However, in certain exceptional circumstances, publication may be anonymised or delayed.

In other cases – for instance, breaches of national legislation that transposes EU Directives – the ECB can only require the national supervisory authorities to open a sanctioning procedure with a view to taking action to ensure that appropriate sanctions are imposed by the national authorities.

The ECB imposes its sanctions in accordance with the ECB Sanctioning Regulation. This Regulation, among others, sets forth the procedural rules and time limits for the imposition of sanctions, as well as their judicial review.

---

20 E.g., requiring a credit institution to hold own funds in excess of the EU law capital requirements or to use its net profits to strengthen its own funds, requesting the divestment of activities that pose excessive risks to the soundness of an institution, limiting variable remuneration when it is inconsistent with the maintenance of a sound capital base, or removing members from the management of a credit institution.


23 The sanctions that the ECB can impose in this case consist of a maximum of twice the amount of the profits gained or losses avoided because of the breach where those can be determined, or a maximum of 10 per cent of the total annual turnover of that institution in the preceding business year. If the institution is a subsidiary, then the relevant total annual turnover is calculated on a consolidated basis.

24 The sanctions that the ECB can impose in this case consist of (1) fines of a maximum of twice the amount of the profits gained or losses avoided because of the infringement where these can be determined, or 10 per cent of the total annual turnover of the undertaking, and (2) periodic penalty payments of a maximum of 5 per cent of the average daily turnover per day of infringement. Periodic penalty payments may be imposed in respect of a maximum period of six months from the date stipulated in the decision imposing the periodic penalty payment.

iii Data protection

To enforce any breach of the provisions of the GDPR, national supervisory authorities are granted a range of corrective powers, such as:

- **a** issuing warnings that intended processing operations are likely to infringe the GDPR and if such processing has taken place and infringed the GDPR, issuing reprimands;
- **b** ordering the controller or processor to comply with a data subject’s request to exercise his or her rights pursuant to the GDPR or to bring processing operations into compliance with the provisions of the GDPR, where appropriate, in a specified manner and within a specified period;
- **c** imposing a temporary or definitive limitation including a ban on processing and to order the suspension of data flows to a recipient in a third country or to an international organisation; and
- **d** imposing an administrative fine, in addition to, or instead of the abovementioned measures, depending on the circumstances of each individual case.

Under the GDPR, national supervisory authorities may impose administrative fines up to €20 million or up to 4 per cent of the total worldwide annual turnover of the preceding financial year of an undertaking, whichever is higher.26 As of early 2020, after 20 months of entry into force of the GDPR, GDPR regulators have already issued hundreds of fines for amounts totalling several hundreds of millions of euros. While such fines have caught a lot of attention, the impact of the other corrective powers should not be underestimated, such as banning a processing activity or ordering the suspension of data flows outside the EU.

---

26 European guidelines have been adopted in relation to the method for determining the amount of fines. See the Guidelines on the application and setting of administrative fines for the purpose of Regulation 2016/679, The Article 29 Data Protection Working Party, 3 October 2017, WP253.
<p>I INTRODUCTION</p>

The main enforcement authorities empowered to investigate and prosecute corporate misconduct are the public prosecutors and investigative magistrates as regards the investigation stage of a criminal procedure, and the criminal courts with regard to adjudication. The police perform investigative measures, including dawn raids or searches, but only following magistrates’ orders.

Argentina is a federal country. The federal government shares its responsibilities with 24 electoral districts, comprising 23 provinces and the autonomous city of Buenos Aires. By constitutional design, the provincial governments have authority over criminal procedure law, so the procedural model varies across the country. Federal offences (including corruption and money laundering) are subject to the federal jurisdiction, where the criminal investigation is still in charge of an investigative magistrate who has the power to delegate this task to the prosecutor – an inquisitorial-oriented procedural model.

A new Criminal Procedure Code establishing an adversarial model, in which prosecutors investigate under judges' control and adjudication, was approved by the National Congress on 6 December 2018. However, it is being gradually implemented, and only a few provinces are already using it. In most provinces, adversarial procedures are already in force for non-federal offences. In this chapter, unless otherwise stated, we refer to federal criminal procedure law.

Although the judiciary and Public Prosecutor's Office (MPF) are independent constitutional powers, specialised literature has shown that both federal prosecutors and judges behave strategically, especially with regard to public corruption or politically sensitive cases.

Currently, corporate conduct can only be criminally prosecuted for some corruption offences (e.g., bribery, trading in influence, illicit enrichment) and economic offences (e.g., money laundering, terrorist financing, insider trading, tax offences, customs offences and foreign exchange offences).

For the prosecution of corruption and economic offences, the Prosecutor’s Office for Economic Criminality and Money Laundering (PROCELAC), a specialised body within the MPF, may become involved. Further, although only empowered to investigate public officials – not corporate wrongdoing – the investigative capacities and participation in criminal proceedings of the Office of Administrative Investigations (PIA) within the MPF,
Argentina and Anti-Corruption Office within the Ministry of Justice and Human Rights (AO), may have an impact in the investigation of corporate conduct. The Financial Intelligence Unit (FIU) may also act as a ‘private prosecutor’ in money laundering investigations.

There is no legal obligation for companies to cooperate with the enforcement authorities. The Argentine legal tradition is unfamiliar with public-private cooperation in criminal investigations, but this could change with the Corporate Criminal Liability Law No. 27,401, which entered into force in March 2018, establishing corporate criminal liability for specific corruption offences. Law No. 27,401 acknowledges internal investigations as an element of compliance programmes, and incentivises cooperation by allowing leniency agreements (similar to deferred prosecution agreements or non-prosecution agreements in the United States) and sanctions mitigation in exchange.

II CONDUCT

i Self-reporting

Legal entities are not legally obliged to self-report when they discover internal wrongdoing, but recent legislation encourages corporations to self-report by providing immunity under certain conditions.

Under Section 9, Law No. 27,401, corporations will be exempted from penalties and administrative liability when three conditions are met:

a the corporation self-reports the offence as a consequence of internal detection and investigation;

b a proper control and supervision system (i.e., a compliance programme, requiring wrongdoers efforts to breach it) had been established before the facts under investigation; and

c proceeds of crime are returned (disgorgement).

If the tribunal does not consider all three conditions fulfilled, self-reporting should be taken into account as a mitigating factor when assessing the penalty.²

Additionally, Antitrust Law No. 27,442 (the Antitrust Law) provides that any individual or legal entity who has committed or is committing any of the offences listed in Section 2 of such law may disclose and acknowledge such conduct before the Competition Tribunal in exchange of an exemption or reduction of the sanctions set forth in the Antitrust Law. The Competition Tribunal will establish a system to determine the order of priority of the applications to benefit from the leniency program.

In order to enjoy the benefits set on the Antitrust Law, the person reporting the wrongful conduct must have performed or be currently performing the action prescribed by the law, and immediately cease to perform it, unless the antitrust authority requests the applicant to continue with the practice or wrongful conduct disclosed to preserve the investigation.

The availing of the exemption benefit or the reduction of the sanctions or fines, as appropriate, cannot be performed jointly by two or more parties that took part in the coordinated practice. However, if a legal entity is self-reporting the wrongful conduct, the directors, managers, administrators, trustees or members of the supervisory board, agents or legal representatives of such legal entity who are involved may avail of the benefits.

² Section 10 of Law No. 27,401.
Self-reporting must be filed before receiving the notice established in Section 41 of the Antitrust Law (the ‘indictment’). This means that the interested party may be involved in a conduct investigation from the beginning (and file its preliminary defence, such as, relevant explanations and continue being investigated during the administrative proceeding stage). The applicant must fully, continuously and diligently cooperate all the time with the antitrust authority.

Pursuant to Section 60(d) of the Antitrust Law, the Competition Tribunal shall keep the applicant’s identity confidential. Furthermore, the declarations, acknowledgements information or any other means of evidence that had been submitted to the Competition Tribunal cannot be disclosed.

Moreover, under the leniency programme set forth in the Antitrust Law, those who have committed and self-reported any anticompetitive behaviour provided therein shall obtain a reduction or be exempted from penalties established in the Antitrust Law, and from the prison penalties that may be applicable to them in any case for having committed any of the offences set forth in Sections 300 and 309 of the National Criminal Code.

However, the Secretary of Domestic Trade (which is the current antitrust authority until the Competition Tribunal is in place and duly functioning) has not regulated the operative details of its leniency program. Therefore, there are no clear rules on how the applicant protection framework will be enforced yet.

In short, there is no legal obligation in Argentina to self-disclose internal wrongdoing. In corruption and antitrust matters, the new legal framework attempts to incentivise this way of cooperation by offering immunity or lenient treatment, depending on the conditions fulfilled, which will be assessed by the enforcement authorities.

Two exceptions to the lack of obligation to self-report should be taken into account:

a In application of the transparency regime of publicly traded corporations, according to Section 99a of the Stock Market Act, companies that are publicly listed before the National Securities Commission (CNV) must disclose to the same authority any fact or situation that could substantially affect the placement of securities of the issuer, the course of the securities’ trading or the development of its activities – including internal wrongdoing.

b Public servants have the duty to report offences that are known to them in the exercise of their public functions.3 This is particularly important for directors of state-owned enterprises or government-appointed directors in businesses in which the state is a minority shareholder, who have been considered public officials by courts.

ii Internal investigations

Law No. 27,401 establishes that corporations may conduct internal investigations with due respect of the rights of the persons under investigation and impose effective sanctions in case of violations to internal policies or applicable laws. This is the first legal recognition to internal investigations as a relevant element of corporate compliance programmes in the Argentine legal system.

As stated in the AO Guidelines for the Implementation of Integrity Programs,4 if a company decides to conduct an internal investigation, it is essential to achieve a balance

---

3 Article 177 of the Criminal Procedure Code.
between the right to investigate and the protection of privacy and personal dignity, and particularly to observe the limits arising from employees’ rights,\(^5\) and that the information management complies with the rules on gathering and handling personal information.\(^6\)

It is, therefore, important that internal investigation actions respond to a written internal protocol previously approved by the board, and previously communicated and agreed upon in writing. Such agreement must include entitling the company to access the sources and devices provided to the employees to perform their work. Employees must be warned about the fact that information stored in such sources is the property of the corporation and that no privacy is to be expected in case such sources are used for personal or illicit purposes.

It is also advisable that the investigations protocol regulates areas such as the chain of custody of the gathered information, how electronic evidence should be handled, and witness interviews, among others.

When conducting witness interviews, the involved employee has the right to retain his or her own counsel, although this is uncommon, especially when the company has a robust investigation protocol.

The procurement of external counsel to conduct the investigation is advisable, especially when the allegations involve senior management, are particularly serious or may have severe reputational consequences. Retaining outside counsel contributes to strengthening the independence and the credibility of the investigation process and enhances attorney–client privilege.

Law 23,187, which regulates the requirements for lawyers to practice law in the City of Buenos Aires (each province of Argentina has its own bar association and regulations but all of them have similar provisions), states that lawyers have the obligation to preserve the attorney–client privilege, unless it is waived by the client. Additionally, Section 7 of Law 23,187 establishes that lawyers have the right to the inviolability of the law firm, safeguarding the constitutional right of defence in court.

Further, according to Section 244 of the Criminal Procedure Code, lawyers are forbidden from testifying in court regarding any information received from the client.

To ensure attorney–client privilege, it is important to state in advance that a conversation or document is privileged and confidential; for example, labelling the documents with the attorney’s name and establishing that the document is ‘private and confidential’.

The privilege does not apply for accountants, so companies should bear in mind that to ensure confidentiality it is advisable to always retain an attorney.

As to the Antitrust Law, it is also advisable that the leniency must be filed by the company. Once an internal investigation detected an antitrust violation, the company’s aim must be to file for the leniency programme before any other person (involved in the internal investigation).

In any case, internal investigations are a new feature in Argentine domestic law. The current state of case law is weighted in favour of employees owing to Argentina’s robust labour and data privacy protections. But it is expected that case law will grow in the coming years on issues related to privacy, legal privilege, the admissibility of evidence obtained in an internal investigation or disciplinary measures, as a consequence of the entering into force of Law No. 27,401.

---

\(^5\) Sections 70 and 72 of the Employment Contract Law.

\(^6\) Section 43 of Argentina’s Constitution and Law 25,236.
iii Whistle-blowers

Because the legal framework has not incentivised whistle-blower reports until very recently, this figure has been almost foreign to domestic investigations. This started to change in late 2016 with the entering into force of two pieces of legislation offering reductions in the threatened punishments to defendants and economic awards to witnesses.

On the one hand, Law No. 27,304 on cooperators (the Repentant Law), foresees that persons investigated for corruption and other complex crimes (except high-ranking state officials) may obtain a reduction of their punishment and the avoidance of prison during the process in exchange of the disclosure of precise, useful and verifiable data relating to other participants in the offence that occupied a higher hierarchical role in the criminal organisation.

Even though the Repentant Law has some limitations (the ‘repentant’ cannot receive immunity but only a reduction of the punishment; and the agreement on the reduced sentence will only be applied by a tribunal that didn’t take part in the negotiations after an oral trial that the defendant cannot avoid), it has been applied, and provided great visibility to the anticorruption agenda especially in the context of the Notebooks scandal, where multiple businessmen and former public officials reached cooperation agreements boosting the investigations.

On the other hand, Law No. 27,319 allows for the application of special investigative techniques in complex crimes investigations, including the possibility of offering economic awards to whistle-blowers.

Anonymous reporting lines have been opened in recent years by the PROCELAC and the PIA, at the MPF, and by the Anti-Corruption Office at the Executive. Moreover, different administrative agencies have opened anonymous reporting lines, such as the Tax Administration and the Agri-Food Sanitary Agency (Senasa).

Further, a National Witness Protection Programme has been in place in Argentina since 2003 (Law No. 25,764). Even though the programme’s resources are limited, and protective measures have been considered weak, in recent years it has offered effective protection to several witnesses of grand corruption cases. The programme sets forth several protection measures, including: (1) personal or domiciliary custody; (2) temporary accommodation in reserved places; (3) change of address; (4) provision of economic means for lodging, transportation, food, communication, healthcare, moving, labour reintegration, security systems, and other essential expenses, inside or outside the country (although for no more than six months).

When it comes to corporate internal whistle-blowers, Law No. 27,401 encourages companies to establish a procedure for internal reporting so that employees and third parties may file reports under confidentiality or anonymously and without fear of retaliation.

Resistance to whistle-blowing is still prevalent in Argentina, so legal and corporate incentives to come forward and cooperate with information need to be sustained in time, together with effective anti-retaliation measures, to overcome this cultural trait. Furthermore, relevant authorities of the current government (that took office in December 2019), including the head of the AO, have publicly discredited the Repentant Law and the practice of rewarding whistle-blowers when claiming that the prosecution of former officials of previous administrations had been a practice of the ‘lawfare’.
### ENFORCEMENT

#### Corporate liability

Companies can be subject to criminal liability according to several provisions of the Argentine Criminal Code (ACC) and various additional laws. The main offences for which companies could be criminally liable for the conduct of its employees are:

- **a** certain corruption offences (Law No. 27,401);
- **b** money laundering (Section 304 and 313, ACC);
- **c** terrorist financing (Section 306 and 313, ACC);
- **d** insider trading (Sections 307–8 and 313, ACC);
- **e** manipulation of financial markets and misleading offers (Section 309 and 313, ACC);
- **f** other financial market offences (Sections 310–11 and 313, ACC);
- **g** customs offences (Customs Criminal Law No. 22,415);
- **h** offences against the foreign exchange regime (Law No. 19,359);
- **i** tax offences (Criminal Tax Law No. 27,430);
- **j** offences against the social security system (Law No. 24.241); and
- **k** collusive conducts (not criminal but administrative corporate liability is foreseen in the Antitrust Law).

The above-mentioned laws establish vicarious corporate liability systems, by which the corporate body is held liable for the illicit actions committed (in most offences by specifically designated persons like the legal representatives, directors or managers; in corruption offences by any person including third parties) with the intervention of the entity or on its behalf, or in its interest or benefit.

Corporate or business fraud and other illicit behaviour can also give rise to civil liability for damages.

Generally, according to Section 1749 of the Civil and Commercial Code (CCC), those who breach an obligation and cause unjustified damage by action or omission are directly liable. Specifically concerning fraud, a company could be liable under Section 271 of the CCC for fraudulent misrepresentation if there is an untrue assertion or concealment of the truth or an artifice, cunning act or contrivance directed to such ends. Additionally, as per Section 338 of the CCC, unsecured creditors have the right to revoke acts carried out by the debtor that infringe on their rights, where an act of corporate or business fraud results in insolvency proceedings. The following elements are necessary: (1) the debtor must be in a situation of insolvency (interruption of payments); (2) the damage caused to the creditor must have resulted from the act of the debtor, or because of the situation of prior insolvency; and (3) the debt must have existed before the debtor's actions.

Besides, Emergency Decree 62/2019 sets a Procedural Regime for Civil Action for non-conviction based asset forfeiture. The Decree sets out a civil action in favour of the federal government, which applies to the goods or titles that are allegedly the result of certain crimes, including bribery. This civil proceeding is autonomous from any conviction issued by a criminal court. The final judgment will be *res judicata* regarding the goods or rights involved, regardless of the outcome of any other judicial action. However, a criminal final judgment of dismissal or acquittal based on the inexistence of the facts under investigation or in its lawfulness obliges the federal government to restore the property or right (or, when that's impossible, an equivalent value in money) to its previous owner.

Additionally, Section 59 of the Argentine General Companies Law No. 19,550 established the duty of directors or managers to act with loyalty and with the diligence of...
a good businessman. Failure to comply with this duty can give rise to unlimited joint and several liabilities for the damages caused to the company, the shareholders and other third parties (among others, any creditors), by their actions or omissions.

Most Argentine large corporations are family owned. The protection of employees by providing and costing their counsel is quite rooted in their practices. However, in light of the incentives set forth in Law No. 27,401, conflict could arise between the interests of the company and those of the employees under investigation for the same facts. The company could mitigate its responsibility by cooperating with the authorities in the identification of the involved employees; and high-rank executives may attempt to divert the internal corporate investigation to hide their own individual responsibilities. When the interests of the legal person and those of its employees may conflict, legal representation should not be exercised by the same counsel.

Pursuant to Antitrust Law, whistle-blowers who have committed any of the offences provided for in Sections 300 and 309 of the ACC shall be exempted from penalties established in such regulation and from the prison penalties that may be applicable to them in any case for having committed any anticompetitive behaviour.

ii Penalties

Although each of the criminal offences mentioned in Section III.i carry their specific penalties, the catalogue of sanctions mainly comprises:

a  fines up to 10 times the value of the goods that have been the object of the offence in money laundering, terrorist financing, insider trading, and other financial markets offences, and between two and five times the amount of the illicit benefit in corruption offences;

b  debarment from government contracting and disqualification from professional practice, or suspension of licence;

c  partial or total suspension of activities for up to 10 years;

d  suspension from participating in state tenders of public works or services, or in any other activity linked to the state for up to 10 years;

e  dissolution and liquidation of the business when it has been created for the sole purpose of the commission of the offence, or when those acts constitute its main activity;

f  loss or suspension of state benefits; and

g  publication of an excerpt of the conviction sentence.

Sanctions are only applied by courts under a final judgment. Nevertheless, courts may order precautionary measures against business defendants, including seizing and freezing of assets (embargo) to guarantee an eventual confiscation.

In addition, as described above, civil forfeiture sanctions may be imposed pursuant to Executive Decree 69/2019 regardless the existence of a criminal conviction.

Pursuant to the Antitrust Law, residual fines applicable under the Antitrust Act were increased and currently amount to 8.122 billion Argentine pesos for anticompetitive practices; 30,457,500 Argentine pesos per day to penalise the breach of (1) timely...
notification of a merger; (2) conditions settled by the competition authorities to cease or avoid several practices; (3) compromises to cease a certain practice; and (4) an order to cease anticompetitive practices.

iii Compliance programmes

Although legal entities are not required under Law No. 27,401 to implement a Compliance Programme, having an effective programme in place may benefit the company.

As explained in Section IV.i, corporations will be exempted from penalty and administrative liability when three circumstances concur simultaneously:

a the legal person self-reports the offence as a consequence of internal detection and investigation;
b before the facts under investigation occurred, an adequate control and supervision system had been established (i.e., a compliance programme); and
c any crime proceed is returned (disgorgement).

Besides, according to Section 8 of Law No. 27,401, courts will take into account the internal proceedings of the legal entity to graduate the penalty. And it will also be relevant if a company spontaneously reports irregularities revealed by an internal investigation.

On the other hand, having a compliance programme is a requisite for contracting with the federal government in contracts that:

a owing to their amount must be approved by a minister or other authority of equivalent hierarchy (at the time of writing, 165 million or 104 million Argentine pesos, depending on the type of contract, today fixed between US$2.32 million and US$1.5 million according to the current Argentine peso–US dollar exchange rate); and
b are included in Section 4 of the Delegated Decree No. 1023/01 (e.g., purchase, supply, services, leases, consultancy, rent with option to purchase, swaps, concessions on the use of goods that belong to the public and private domain of the nation state) or are governed by Laws Nos. 13.064 (on public works), 17.520 (on the concession of public works) and 27.328 (on public-private partnerships) and public utility concessions or licence contracts.

To be considered adequate under Sections 22 and 23 of Law No. 27,401, a compliance programme must:

a be appropriate to the specific risks, size and economic capacity of the legal entity;
b include a code of ethics and internal policies to prevent offences in any interactions with the public sector; and
c lay out periodic compliance training to directors, administrators and employees.

Additionally, the programme may contain the following elements:

a periodical risk assessment and consequent adaptation of the programme;
b visible and unequivocal support from senior management (‘tone at the top’);
c internal channels to report irregularities, open to third parties and adequately publicised;
d a whistle-blower protection and anti-retaliation policy;
e an internal investigations system that respects the rights of those under investigation and imposes effective sanctions for breaches to the code of conduct;
procedures that attest the integrity and track record of third parties or business partners, including suppliers, distributors, service providers, agents and intermediaries, upon contracting their services and during the commercial relationship;

M&A due diligence;

monitoring and continuous evaluation of the programme’s effectiveness;

an internal authority in charge of its development, coordination and supervision; and

compliance with the statutory specific requirements issued by the national, provincial, municipal or communal levels of government.

iv Prosecution of individuals

Law No. 27,401 establishes that the criminal responsibility of corporations is independent from that of the individual offenders, and that businesses can be convicted even if no individual has been identified or judged, as long as it is found that the offence could not have been committed without the tolerance of the corporate body. This rule, and the incentives provided for cooperation, are designed to stimulate both businesses and the individuals to come forward and cooperate with the authorities in the identification of responsibilities.

In this context a conflict may arise between the company and its employees; see Section III.i.

In the context of a business cooperation strategy, an internal investigation and the enforcement of disciplinary measures are advisable, as well as an internal reorganisation to avoid the repetition of the identified wrongdoing in the future.

IV INTERNATIONAL

i Extraterritorial jurisdiction

Section 258-bis of the ACC criminalises the active bribery of foreign public officials. Additionally, Law No. 27,401 foresees that corporations are criminally liable for this offence. The elements of the offence are as follows: offering or giving money or any object of pecuniary value, or other benefits such as gifts, favours, promises or benefits, to a foreign public official for his or her benefit or the benefit of a third party, in an economic, financial or commercial transaction. A foreign public official is defined under Argentine law as a public official of another state or territorial entity recognised by Argentina, including those appointed or elected to perform a public function in government or any class of body, agency or public company where said state exerts a direct or indirect influence.

The enforcement of this offence is weak in Argentina. At the time of writing, nine investigations have been opened for foreign bribery. No conviction was yet reached, and only one indictment was decided.8

ii International cooperation

Argentina collaborates with foreign authorities in investigations as a member of bilateral, regional and multilateral treaties. For example, Law No. 26,004 on the Mutual Assistance Agreement in Criminal Matters of Mercosur, Bolivia and Chile, and Law No. 26,139 on the Inter-American Convention on Mutual Legal Assistance in Criminal Matters. For countries

that do not share a treaty with Argentina, Law No. 24,767 on International Cooperation in Criminal Matters applies. This law also regulates the general provisions of extradition, and other forms of assistance in the investigations of crimes. In addition, the FIU (as a member of the Egmont Group), and the Federal Administration of Public Revenues exchange data on a regular basis with their foreign counterparts.

iii Local law considerations

The investigation conduction could imply having access and process ‘personal data’ (as broadly defined by the Argentine Personal Data Protection Law No. 25,326 (APDPA)), therefore certain aspects from the Argentine Data Privacy should be taken into account.

The APDPA sets forth a strict data protection system aimed at regulating the collection, storage and use of databases and personal data which is stored or processed – even on a temporary basis – in Argentina, to allow data subjects to monitor the usage of their information, and as a consequence it states general guidelines for the legal usage and treatment of personal information.

Under the APDPA, personal data transferring to countries not granting adequate levels of protection is in principle prohibited. However, it is admitted if: (1) data subjects give their express consent to said transferring; (2) the adequate protection levels arise from contractual clauses, binding corporate rules, or self-regulation systems of the data assignor and data assignee; or (3) the data transferring is because of an exception provided by law (i.e., judicial international cooperation; banking or capital markets transactions authorised by applicable law; and international transfer taken place in the framework of international treaties to which Argentina is part).

From a strictly labour law standpoint, the general principle is that employees may legitimately consider that their emails (specifically those unrelated to their work) are private and not meant to be read by any other person. Therefore, for companies to lawfully monitor and audit their employees’ email accounts (as a tool provided by the employer), it should be necessary to previously inform the employees about the company’s policy and the method of monitoring. To ensure that the employer’s monitoring rights and employees’ privacy rights are balanced, companies shall make a cautious and properly articulated use of their rights and powers, which could be broadly defined in corporate guidelines or policies.

Therefore, it is usually understood that corporate policies on the matter should clearly establish that email accounts are of the exclusive and sole property of the company and can only be used for working purposes. Accordingly, their personal use should be considered a misconduct.

Lastly, there are no specific provisions as to the circumstances under which foreign protections for attorney–client communications are recognised in Argentina. However, by virtue of constitutional rights and public and private international law, foreign attorney–client privilege should be valid in Argentina to at least the same extent as local protections. Nevertheless, it is advisable to engage local counsel to secure these protections.

V YEAR IN REVIEW

Recent years had shown a peak in anti-corruption and anti-money laundering enforcement, boosted by both legal and regulatory reforms and a changing political environment both at the national and regional levels. High-ranking officials of former administrations were
prosecuted on corruption and money laundering charges, including former President Cristina Kirchner. Law enforcement reached not only former officials but also private sector executives.

In 2019, several high-profile investigations of alleged corruption during the former governments were sent to trial. In addition, former Secretary of Public Works, José López, was sentenced to six years in prison and disqualification for life for illicit enrichment.

In October 2019, former head of cabinet to Nestor and Cristina Kirchner’s administrations, Alberto Fernandez, was elected President, and former President Cristina Kirchner was elected Vice-president. After the elections, several former authorities and businessmen who had been imprisoned in the context of corruption investigations were released from prison. The current administration portrays those corruption investigations, carried out under a government of a different political sign, as instances of the ‘lawfare’. Such investigations are still open and some of them have been sent to oral trial.

The new head of the Anticorruption Office has publicly criticised both Law 27,401, on criminal corporate liability for corruption offences, and the ‘Repentant law’. The former was pointed as foreign to the Argentine criminal law tradition, while the latter was depicted as an extortionate tool, which has been used as a means for ‘lawfare’.

In addition, President Alberto Fernandez announced a reform to the federal criminal justice system, the details of which are still to be publicised and debated.

VI CONCLUSIONS AND OUTLOOK

Anti-corruption and anti-money laundering enforcement have shown a peak in recent years. New legal and regulatory frameworks in both areas, as well as in antitrust matters, have left multiple open questions that have still not received answers through adjudication. To date, there is no public information on any application for a leniency programme filed on antitrust matters, neither that any company has been yet charged on the grounds of Law 27,401.

In such context, a new administration took office in December 2019. Former head of cabinet to Nestor and Cristina Kirchner’s administrations, Alberto Fernandez, was elected President, and former President Cristina Kirchner was elected Vice-president. The current administration portrays the corruption investigations that were carried out in recent years, under a government of a different political sign, as instances of the ‘lawfare’. The President announced that it will promote a reform to the federal criminal justice system with the objective of avoiding its political use. However, the rapid hit of the covid-19 pandemic impeded the new government from showing a clear orientation on criminal and compliance enforcement, and no formal project to reform the current legal framework has yet been presented.
I INTRODUCTION

The Australian government has empowered a number of regulatory bodies to investigate and prosecute corporate misconduct. These are:

a. The Australian Securities and Investments Commission (ASIC) is the main corporate regulator. It enforces and regulates company law.

b. The Australian Competition and Consumer Commission (ACCC) enforces and regulates competition and consumer laws.

c. The Australian Tax Office enforces and administers the federal taxation system and superannuation law. It is Australia’s principal revenue collection agency.

d. The Australian Transaction Reports and Analysis Centre (AUSTRAC) is the national financial intelligence agency. It enforces anti-money laundering and counter-terrorism financing laws.

All these regulatory bodies have, in some form, compulsory powers that can require individuals and companies to produce documents and information, including attendance at compulsory examinations where there is no privilege against self-incrimination. They also encourage cooperation when exercising their investigative functions.

When a matter is referred for criminal investigation, it is often investigated by the Australian Federal Police (AFP), the national law enforcement agency. The AFP is solely responsible for investigating contraventions of Commonwealth criminal law. The Commonwealth Director of Public Prosecutions (CDPP), the national prosecutorial agency, is in turn responsible for the prosecution of alleged offences against Commonwealth law.

When Australian legal practitioners conduct an internal investigation, it is likely to be in the context of a regulatory probe by one of these Australian government bodies, which may also include a concurrent criminal investigation by the AFP.

---

1 Dennis Miralis and Phillip Gibson are partners and Jasmina Ceic is a senior associate at Nyman Gibson Miralis.
II CONDUCT

i Self-reporting

Australian regulators have had long-standing formal mechanisms in place for self-reporting of both civil and criminal wrongdoing. The AUSTRAC, the ACCC and the ASIC, for example, all have specific mechanisms for self-reporting, whether it be mandatory or voluntary. The ASIC, in particular, relies heavily on self-reporting to fulfil its regulatory oversight of the financial services sector. If a corporate cooperates with the ASIC, it can:2

a fully recognise that cooperation (taking into account whether the corporate has a self-reporting obligation);
b negotiate alternative resolutions to the matter;
c take into account the degree of cooperation provided during the investigation when determining the type of remedy or remedies sought, depending on all the circumstances of the case;
d in administrative and civil matters (other than civil penalty matters), make particular submissions to the tribunal or court as to what the outcome should be;
e in civil penalty matters, take the corporate’s cooperation into account; and
f in criminal matters, take the corporate’s cooperation into account.

A notable development in self-reporting is the recent formalisation of policy concerning foreign bribery, reflective of Australia’s ever-growing presence on the international stage. On 21 December 2017, the AFP and the CDPP released a joint guideline clarifying the principles and process that apply to corporations who self-report conduct involving a suspected breach of Division 70 of the Criminal Code 1995 (Cth).3

Division 70 of the Criminal Code is concerned with the bribery of foreign public officials. Section 70.2 provides for the offence of bribing a foreign official. Contraventions of Section 70.2 carry significant penalties for an individual or corporation (up to 10 years’ imprisonment and a fine of 10,000 penalty units for an individual, 100,000 penalty units for a corporation or three times the value of the benefit provided or 10 per cent of the corporation’s annual turnover over a defined turnover period). Presently, there is no obligation to self-report suspected breaches of Division 70 of the Criminal Code.

Although self-reporting is not mandatory, providing full and frank disclosure and assistance to investigating authorities is an appropriate action following the discovery or detection of a contravention of Section 70.2. There are, as the guideline suggests, many reasons why a corporate would choose to self-report wrongdoing:4

a to proactively identify and address wrongdoing within the company;
b to comply with directors’ statutory and fiduciary duties to act in the best interests of the company;
c to limit corporate criminal liability;
d to minimise reputational damage;
e to demonstrate a cooperative intent with the AFP in investigating the conduct;

---

2 ASIC Information Sheet 172 (INFO 172), issued in May 2015.
3 AFP and CDPP Best Practice Guidelines: Self-reporting of Foreign Bribery and Related Offending by Corporations.
4 ibid.
The guideline suggests that assistance which the corporate entity could provide would include the provision of reports prepared by the corporation or its lawyers to investigators, and access to any witnesses that may ultimately give evidence in court. Assistance has its clear benefits; the corporation can be given an undertaking that evidence given by the corporation as a witness is not admissible, whether directly or derivatively, against the corporation in any civil or criminal proceedings.\(^5\) The corporation can also be given an indemnity from prosecution, but this indemnity does not prevent a proceeds of crime authority from commencing civil confiscation proceedings under the Proceeds of Crime Act 2002 (Cth).

The implementation of the guideline is in line with Australia’s overall commitment to combat foreign bribery. Australia is a signatory to the Organisation for Economic Co-operation and Development’s (OECD) Anti-Bribery Convention. A Phase 4 review of Australia’s implementation of the Anti-Bribery Convention occurred in December 2017. The report following the Phase 4 review detailed several recommendations that indicate the Australian government’s increased commitment to detecting and prosecuting foreign bribery. These include:\(^6\)

\(a\) improving the potential for detecting foreign bribery through Australia’s anti-money laundering system;
\(b\) enhancing whistle-blower protection for private sector employees;
\(c\) continuing to investigate and prosecute foreign bribery and ensuring appropriate resourcing of authorities to facilitate those improvements; and
\(d\) engaging with the private sector to encourage adoption of robust anti-bribery procedures.

Consistent with this approach are the measures set out under the ‘Draft guidance on the steps a body corporate can take to prevent an associate from bribing public officials’ consultation paper released by the Attorney General of Australia in November 2019. On 2 December 2019, the Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2019 was introduced into Parliament. While the Bill is set to introduce a new corporate offence for failure to prevent a foreign bribery offence, commissioned by an associate of a body corporate, under Section 70.5A the Criminal Code Act 1995 (Cth), it also includes a proposed defence if the body corporate can demonstrate it had adequate procedures in place to prevent such an offence. Following consideration of feedback received from relevant stakeholders in February 2020, the Attorney General intends to publish a final guidance paper to coincide with the introduction of the amending legislation.

ii Internal investigations

Established on 14 December 2017, the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry has shed light on the practices and culture of the financial services industry, revealing inadequacies in the investigative and reporting practices adopted by some of Australia’s largest corporate entities. Common criticisms

\(^5\) ibid.
\(^6\) Implementing the OECD Anti-Bribery Convention Phase 4 Report: Australia.
levelled at these entities concern the delay in reporting misconduct, general obscurification, misleading behaviour and interference with functions of the corporate regulator, and questionable ‘independent reporting’ by law firms retained to conduct internal investigations and respond to regulatory probes.

The final report of the Commissioner, the Honourable Kenneth M Hayne AC QC, was submitted on 1 February 2019. The report included 76 recommendations relating to the conduct of banks, mortgage brokers, financial advisers and superannuation trustees as well as Australia’s financial services regulators. The Commissioner invited ASIC to investigate 11 potential instances of criminal misconduct, with the view of instigating criminal or other legal proceedings as appropriate. The report stressed the need for supervisory bodies such as the Australian Prudential Regulation Authority and ASIC to build a supervisory programme ‘focused on building culture that will mitigate the risk of misconduct’.7

Following the release of the final report, ASIC announced that would establish an internal ‘Office of Enforcement’, creating a separate department for enforcement staff with a specific focus on court-based outcomes.8 The ASIC Office of Enforcement is now established and is operational following a A$404 million federal government investment package. A marked shift towards increased investigation and litigation by the agency is evidenced by a 20 per cent increase in ASIC enforcement investigations and a 206 per cent increase in wealth management investigations between July 2018 and June 2019. This trend of increased enforcement by way of litigation is set to continue in the foreseeable future. Between 1 January 2019 and 30 June 2019, ASIC expressly targeted contraventions in the following areas, said to be of primary concern:

a harm caused by corporate gatekeepers, including auditors and liquidators, who hold positions of responsibility and trust, and who must lawfully discharge the obligations their positions carry;
b dishonest, misleading and deceptive conduct by those providing financial advice or financial services; and
c market misconduct that threatens to create uncertainty and erode investor confidence.9

The inadequacies revealed by the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry illustrate that the decision to investigate can be a difficult one, particularly where there is a grave risk of reputational damage and the consequent erosion in public confidence in the organisation. Of primary concern is whether an internal investigation is required to comply with a relevant law, regulation or corporate policy. A secondary concern must always be the exercise of balancing the costs associated with any internal investigation and the effects of inactivity, delay and failing to investigate.

Commonly, internal investigations are undertaken by a lawyer or team of in-house lawyers. Sometimes, because of the scope or complexity of an investigation, external law firms will be briefed alongside specialist investigators, auditors and accountants. These firms usually specialise in civil litigation and corporate law more generally. However, the emerging understanding of the internationalisation of economic crime may change this paradigm. Advances in digital technology have driven an increase in incidences of white-collar crime and

---

7 Recommendation 5.7, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry.
8 ASIC update on implementation of Royal Commission recommendations, 19 February 2019.
cybercrime. Corporations may think it prudent to use specialist criminal lawyers to provide advice much earlier in the investigation process and, where appropriate, assist in the conduct of the internal investigations. Where there is a concurrent regulatory probe with parallel criminal investigations in multiple jurisdictions, complex transnational criminal issues may arise concerning the right against self-incrimination; the use of the exchange of information and data between jurisdictions for criminal investigation and prosecution; and, if there is a request for extradition, whether dual criminality or double jeopardy are applicable.

In-house lawyers need to be particularly aware of the possibility that an internal investigation can lead to both civil and criminal proceedings, sometimes running concurrently, and sometimes crossing multiple jurisdictions. The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters allows for evidence to be taken through Australian courts for use in a foreign civil proceeding following a request by a foreign court.\(^\text{10}\)

Every state and territory in Australia has legislation that allows for evidence to be taken in this way, and often when such evidence is being sought, it is not uncommon for there to be a criminal investigation already under way. Notably, some protections are preserved under the Convention, the fifth amendment, for example, can be claimed in Australia where the subpoenaed party faces criminal charges in the United States. The use of international mechanisms such as the Hague Convention, when corporations are subjected to both regulatory and criminal prosecutions, is likely to become more prevalent, until such time as an international convention or treaty specifically focusing on economic crime is adopted. In the meantime, substantive legal issues such as mutual assistance across jurisdictions, including adequate safeguards for human rights such as the right to a fair trial and privacy, will need to be considered by the courts on a case-by-case basis, under domestic law’s interpretation of the Hague Convention.

### iii Whistle-blowers

In December 2016, as part of its Open Government National Action Plan, the Australian government made a commitment to ensure that there were appropriate protections for persons reporting corruption, fraud, tax evasion or avoidance and misconduct within the corporate sector.\(^\text{11}\) A year later, on 13 December 2017, the Treasury Laws Amendment (Whistleblowers) Bill 2017 (Cth) was introduced in Parliament, some 13 years after the introduction of legislative protection for whistle-blowers under the Corporations Act 2001 (Cth). The Act has now passed both Houses of Parliament and came into force on 1 July 2019.

The Bill was introduced because of perceived deficiencies with the existing regime; namely, gaps in whistle-blower protection. Statutory protection for some whistle-blowers is non-existent and only piecemeal in other areas, and some protections have not adjusted to reflect the actual remits of regulators.

The amendments to the Corporations Act 2001 (Cth) are designed to advance the government’s goal of encouraging the disclosure of civil and criminal wrongdoing, particularly in the private sector, to improve overall compliance with laws and regulations by corporations. The government considers whistle-blowers to be playing a critical role in uncovering corporate crime, particularly because of the difficulties faced by law enforcement in detecting corporate misconduct.

\(^{10}\) Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters.

\(^{11}\) https://ogpau.pmc.gov.au/.
The Bill creates a single, consolidated whistle-blower protection regime in the Corporations Act 2001 (Cth) and a whistle-blower protection regime in the Taxation Administration Act 1953 (Cth) through various legislative amendments. It also repeals the financial whistle-blower regimes.

The changes to protections in the Corporations Act 2001 (Cth) are overwhelmingly positive. No longer are whistle-blowers required to identify themselves when making a disclosure, and the types of persons and bodies that are allowed to disclose the identity of whistle-blowers have been comprehensively clarified in the Bill. Existing immunities have been extended, the amendments ensuring that information that is part of a protected disclosure is not admissible in evidence against that whistle-blower in a prosecution for an offence (other than in proceedings concerning the falsity of the information).

The remedies available to whistle-blowers who suffer detriment because of a qualifying disclosure in the Corporations Act 2001 (Cth) have been expanded. The Bill creates a civil penalty provision to address the victimisation of whistle-blowers and allows for the criminal prosecution of victimisers. Other remedies, such as compensation, have been simplified. A person can seek compensation for loss, damage or injury suffered as a result of a victimiser’s conduct, where that conduct causes any detriment to another person or threatens to cause detriment to another person, believing or suspecting that a person made, may have made, proposes to make, or could make a qualifying disclosure; and the belief or suspicion is the reason, or part of the reason, for the conduct.

The Bill also addresses corporate governance concerns by introducing a requirement for large proprietary companies and proprietary companies that are trustees of registrable superannuation entities to implement whistle-blower policies. The policies have to detail the protections available to whistle-blowers, how and to whom disclosures can be made, the support that the corporate will offer to whistle-blowers, the corporate’s investigation process and how the corporate will ensure fair treatment of employees mentioned or referred to in whistle-blower disclosures.

The comparable amendments to the Taxation Administration Act 1953 (Cth) introduce protections and remedies for whistle-blowers who make disclosures about breaches or suspected breaches of Australian taxation law or taxation-related misconduct. As with the amendments to the Corporations Act 2001 (Cth), the revised act offers protection for whistle-blowers from civil, criminal and administrative liability in respect of qualifying disclosure, the creation of offences in respect of conduct that causes detriment to a person, and offers a mechanism for court-awarded compensation to persons who suffer damage in respect of a qualifying disclosure.

The Honourable Senator Mathias Cormann (Minister for Finance and Deputy Leader of the Government in the Senate) commented during the second reading of the Bill that the ‘reforms will also improve practices within Australian businesses, including in the areas of corporate governance and integrity. Officers, employees and taxpayers will now be aware that there is a significantly higher likelihood that misconduct will be reported’. The new whistle-blower amendments will align Australia with international developments and it is expected that this will lead to an increase in regulatory and criminal investigations as well as prosecutions of corporations. Time will tell, however, if the Bill will be the catalyst for immediate change.
ENFORCEMENT

Corporate liability

It is expected that Australia's existing corporate liability regime will soon be subject to radical transformation. The Australia Law Reform Commission (ALRC) is presently undertaking a comprehensive review under terms of reference which indicate that broad changes should be expected, aimed to simplify and strengthen the existing statutory provisions that attribute criminal liability to companies in Australia. The Attorney-General of Australia has referred the following matters to the ALRC:

a. the policy rationale for Part 2.5 of the Criminal Code 1995 (Cth);
b. the efficacy of Part 2.5 of the Criminal Code 1995 (Cth) as a mechanism for attributing corporate criminal liability;
c. the availability of other mechanisms for attributing corporate criminal responsibility and their relative effectiveness, including mechanisms which could be used to hold individuals (senior corporate office holders) liable for corporate misconduct;
d. the appropriateness of effectiveness of criminal procedure laws and rules as they apply to corporations; and
e. options for reforming Part 2.5 of the Criminal Code 1995 (Cth), or other relevant legislation to strengthen and simplify the Commonwealth corporate criminal responsibility regime.  

Under the existing regime, civil and criminal corporate liability can be derived from common law or from statute. The standard of proof in civil proceedings is 'on the balance of probabilities', while in criminal proceedings it is 'beyond a reasonable doubt'.

Under common law, a corporation is liable for the conduct and guilty mind of a person or persons who are the directing will and mind of the corporation. Commonly, that person or persons will be the managing director, board of directors or a person who has the authority to act on the corporation’s behalf. Criminal liability can also extend to employees or agents acting within the actual or apparent scope of their employment, if the corporate expressly, tacitly or impliedly authorises or permits the conduct that is the subject of the offence.

Statutory liability is more clearly defined. Chapter 2, Part 2.5, Division 12 of the Criminal Code 1995 (Cth), for example, outlines corporate criminal responsibility as it applies to the Code. The Criminal Code 1995 (Criminal Code) applies to bodies corporate in the same way it applies to individuals (or where provided, with modifications). For the most part, offences under the Criminal Code have physical elements (action or conduct) and fault elements (intention, knowledge, recklessness or negligence). These elements must be satisfied beyond reasonable doubt in order for an offence to be proven beyond reasonable doubt. Notably, a body corporate may be found guilty of any offence under the Criminal Code, including one punishable by imprisonment.

Where a physical element of an offence is committed by an employee, agent or officer of a body corporate acting within the actual or apparent scope of his or her employment, or within his or her actual or apparent authority, the physical element must also be attributed to the body corporate. If intention, knowledge or recklessness is a fault element in relation to

---

a physical element of an offence, that fault element must be attributed to a body corporate that expressly, tacitly or impliedly authorised or permitted the commission of the offence. Authorisation or permissions may be established by various modes of proof.

Other acts of Parliament, such as the Corporations Act 2001 (Cth) and the Australian Securities and Investments Commission Act 2001 (Cth), contain similar liability provisions.

Most criminal conduct is investigated by the AFP and prosecuted by the CDPP.

Two key changes to the existing statutory scheme, proposed by the ALRC include:

a) Expanding the individuals whose conduct may be attributed to the corporate body from ‘officers, employees, and agents’ to ‘associates’ acting on behalf of the corporation. An associate is proposed to be defined as ‘any person who performs services for or on behalf of the body corporate’. Significantly, in addition to employees and agents, this may extend to parties such as contractors and subsidiaries.

b) The introduction of a due diligence defence of which the legal burden of proof rests on the corporation. Currently, a corporation may be either vicariously or directly liable for the actions of its employees, without necessarily having recourse to a due diligence defence in certain situations. The question of whether a corporation has in fact exercised due diligence is a matter of fact which can again be established using various modes of proof.

Comparable defences feature in existing legislative schemes in the United Kingdom, one example being Section 7(2) of the Bribery Act 2010 (UK) which creates a defence where ‘adequate procedures’ are in place to prevent bribery.

The ALRC final report is due on 30 April 2020. While the shift towards more aggressive enforcement action has already commenced, reform focusing on simplification of Part 2.5 of the Code and consolidation of the presently diverse corporate liability regulatory landscape in Australia will further strengthen the overall means by which the regime can be used to attribute corporate criminal liability and create an environment hostile to criminal contraventions on the part of corporate bodies.

ii Penalties

The main form of penalty imposed on a corporate body is a fine.

Statutory fines have defined maximum limits, either expressed by a maximum number of penalty units that can be imposed or by a monetary figure. In a law of the Commonwealth or Territory ordinance, unless the contrary intention appears, one penalty unit amounts to A$210. The quantum of the fine can be significant. For example, if a corporate body is found guilty of the offence of bribery of a Commonwealth public official, the maximum fine that can be imposed is 100,000 penalty units (amounting to A$21 million).

Serious offences can, in certain circumstances, lead to the company being wound up pursuant to Section 461 of the Corporations Act 2001 (Cth). Similarly, serious offences can lead to confiscation proceedings being brought by the AFP pursuant to the Proceeds of Crime Act 2002 (Cth) (the Act). The Act was passed on 11 October 2002 and came into operation on 1 January 2003. The Act provides a scheme to trace, restrain and confiscate the proceeds of crime against Commonwealth law. In some circumstances, it can also be used to confiscate the proceeds of crime against foreign law or the proceeds of crime against State law (if those proceeds have been used in a way that contravenes Commonwealth law). It is expected that the proceeds of crime laws will increasingly be applied to white-collar matters where, in the past, they have been mostly applied to general crime.
The Corporations Act 2001 (Cth) and The Australian Securities and Investment Act (Cth) provide similar sanctions. Notably, a recent review by the ASIC Enforcement Review Taskforce has called for an increase in civil penalty amounts in legislation administered by the Commission: for individuals, 2,500 penalty units (amounting to A$525,000) and for corporations the greater of 50,000 penalty units (amounting to A$10.5 million) or three times the value of benefits obtained or losses avoided or 10 per cent of annual turnover in the 12 months preceding the contravening conduct (but not more than 1 million penalty units (A$210 million)). Additionally, it was recommended that ASIC be provided with similar powers to the AFP and be directly able to freeze and forfeit proceeds of crime.

In response to the review of the ASIC Enforcement Review Taskforce, the Treasury Laws Amendment (Strengthen Corporate and Financial Sector Penalties) Bill 2018 was introduced to Parliament on 24 October 2018 and passed by both Houses of Parliament on 18 February 2019. The legislative response includes reforms that ultimately exceed the penalty regime as proposed by the Taskforce.

Under the amendments to the Corporations Act 2001 (Cth) and the Australian Securities and Investment Act (Cth), the maximum civil penalty amounts for individuals are at least 5,000 penalty units (amounting to A$1.05 million) or three times the financial benefits obtained or losses avoided; and, for corporations, at least 50,000 penalty units (amounting to A$10.5 million) or three times the value of benefits obtained or losses avoided, or 10 per cent of annual turnover in the 12 months preceding the contravening conduct (but not more than 2.5 million penalty units (A$525 million)).

Other penalties include enforceable undertakings, where the company must carry out or refrain from certain conduct. These are not available where the penalty imposed is dealt with by criminal sanction and are only appropriate for minor breaches of the law.

iii  Compliance programmes
A corporate’s compliance programme will be relevant to the corporate’s criminal liability. For example, liability for some offences charged pursuant to the Criminal Code can be established on the basis that the corporate impliedly authorised the offending conduct by failing to create and maintain a culture that required compliance with the relevant provision. The existence of a compliance programme and the exercise of due diligence will be relevant under Section 12.3(3) of the Criminal Code and will be expressly provided for as a defence under the proposed ALRC recommendations considered above.

Notably, a corporation may rely on the defence of mistake of fact pursuant to Section 9.2 of the Criminal Code. The corporate must prove that the corporation had a compliance programme and exercised due diligence.

Additionally, the existence and effectiveness of a compliance programme may be a relevant factor at sentence proceedings, as it can change the court’s assessment of objective criminality of the offence.

iv  Prosecution of individuals
Chapter 2D, Part 2D.1, Division 1 of the Corporations Act 2001 (Cth) provides for the general duties of officers and employees of a corporation. Section 180 imposes a civil obligation of care and diligence; Section 181 imposes a civil obligation to act in good faith in the best interests of the corporation; Section 184 makes it a criminal offence if a director or other officer of a corporation is reckless or intentionally dishonest in failing to exercise their powers and discharge their duties in good faith in the best interests of the corporation or for
a proper purpose. Further, under Section 184, if an employee of a corporation uses his or her position or uses information dishonestly to gain an advantage, he or she is also liable to a criminal penalty.

Whether an individual is prosecuted or not for contraventions of the Corporations Act 2001 (Cth) will depend on the severity and nature of the contravention.

IV INTERNATIONAL

i Extraterritorial jurisdiction

Australia’s corporate and criminal laws have limited extraterritorial application. Typically, the laws will require that the act, omission or person to have some connection with Australia.

The regulation of corporations under the Corporations Act 2001(Cth) extends to foreign corporations who are ‘carrying on business’ in Australia. For example, the power to disqualify individuals under the Corporations Act 2001 is limited to the time when those individuals are managing a foreign corporation, unless the act or omission occurred in connection with the foreign company carrying on business in Australia; or if the act or omission was done or proposed to be done in Australia; or if the act or omission was a decision made by the foreign company whether or not to carry out, or to refrain from doing an act in Australia.

Under the Criminal Code, a person does not commit an offence unless the conduct of the alleged offence occurred wholly or partly in Australia, or the result of the conduct occurs wholly or partly in Australia. However, geographical jurisdiction is extended in certain circumstances; for example, where at the time of the alleged offence the offence occurs wholly outside the jurisdiction of Australia, and the person is an Australian citizen or the person is a body corporate incorporated by or under a law of the Commonwealth or of a state or territory.

ii International cooperation

Australia cooperates with overseas law enforcement and regulatory bodies in a number of ways through both formal and informal channels, across multilateral and bilateral treaties as well as through international conventions.

The ASIC, for example, has agreements with a number of other countries’ law enforcement authorities, which allow for cooperation between countries. These memorandums of understanding enable the exchange of information and for mutual cooperation and assistance to investigations. Australia has such agreements with a wide range of countries, such as Austria, Brazil, China, France and Japan. However, there are some restrictions on the extent to which the ASIC can provide assistance to foreign authorities. Sections 6 and 7 of the Mutual Assistance in Business Regulation 1992 (Cth) require the ASIC to receive authorisation from the Attorney-General prior to obtaining documents and testimony on behalf of foreign authorities.

14 Section 206H, Corporations Act 2001 (Cth).
15 Division 14, Criminal Code 1995 (Cth).
16 Division 15; Criminal Code 1995 (Cth).
International cooperation is also achieved through Australia’s involvement in a number of tax information exchange agreements (TIEAs) as developed by the OECD. These agreements allow for an obligation between Australia and non-OECD countries to assist each other by requesting the exchange of tax information to eliminate the avoidance of tax. The information that can be exchanged is limited to when a specific investigation is occurring. Australia has TIEAs with a number of countries, including The Bahamas, Cayman Islands, Guatemala, Liechtenstein and Vanuatu.

Australia is party to a number of bilateral and multilateral extradition treaties. Extradition requests (either made by Australia or received by Australia) are governed by the operation of the Extradition Act 1988 (Cth). Extradition is used only for serious offences, and most commonly for offences committed against the person.

Australia also has agreements with international law enforcement agencies. In particular, the AFP is part of the International Foreign Bribery Taskforce. The taskforce involves the Federal Bureau of Investigations, the Royal Canadian Mounted Police, the AFP and the United Kingdom’s National Crime Agency working together to provide information and cooperation on cross-border anti-corruption investigations; it allows for the agencies involved to share knowledge, investigative techniques, methodologies and best practice.

iii Local law considerations
Privacy is a major concern when information is shared with overseas entities and authorities. Schedule 1 of the Privacy Act 1988 (Cth) contains the Australian Privacy Principles (APPs). These principles outline that where information is being shared by an APP entity (which includes the AFP and bodies established by a Commonwealth enactment such as the ASIC) to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the principles. However, this principle does not apply where disclosure is required or authorised by an international agreement relating to information sharing, or is reasonably necessary for enforcement-related activities. This means that the principles will not apply in instances such as when the AFP or the ASIC sends information to other regulatory agencies to provide information relevant to ongoing investigations. Currently, there is little jurisprudence in Australia dealing with the proper parameters on the exchange of information across jurisdictions where criminal sanctions may apply. This is an area in which Australian courts may become more involved, as the internationalisation of economic crime has been attended by a significant increase in the dissemination and sharing of information about individuals and corporations with, to date, very little oversight by Australia’s judiciary.

21 Section 6, Privacy Act 1988 (Cth); Australian Privacy Principle 8.1.
22 Australian Privacy Principle 8.2.
V YEAR IN REVIEW

On 23 March 2019, the federal government continued its post-Royal Commission reform measures by announcing a A$35 million investment to extend the federal court’s jurisdiction to cover corporate crime. There have been a number of high-profile cases in various Australian federal and state jurisdictions during the past year across a broad area of white-collar crime offending that has required Australian courts to consider the appropriate sentencing principles and penalties to be applied to corporate offenders. Most of the court cases have involved individuals rather than corporations.

In Commonwealth Director of Prosecutions v Nakhl [2019] NSWDC (Unreported), the defendant was sentenced on 15 March 2019 having entered pleas of guilty of eight counts of engaging in dishonest conduct while carrying out a financial services business under Section 1041G(1) of the Corporations Act 2001 (Cth). Four further counts under the same offence provision where considered on sentence pursuant to Section 16BA of the Crimes Act 1914 (Cth). The offending conduct occurred while Mr Nakhl was acting as a financial adviser and representative of both Australian Financial Services Ltd, which was in liquidation, and SydFA Pty Ltd, which was deregistered.

Mr Nakhl misappropriated and lost approximately A$5.1 million dollars of self-managed superannuation funds, invested by 12 separate clients, in personal and business ventures not authorised by the given investors. Mr Nakhl then furnished false reports to the investors, which indicated that funds had been invested in authorised funds and that the funds were performing to a satisfactory standard.

Following investigation, ASIC initially obtained freezing orders against assets held by Mr Nakhl prior to his declaration of bankruptcy. Mr Nakhl was sentenced to 10 years’ imprisonment with a non-parole period of six years. The sentence represents the longest sentence of imprisonment ever imposed against a financial adviser in Australia.23

Hui (Steven) Xiao v. R [2018] NSWCCA 4 was an appeal to the Court of Criminal Appeal on the severity of a sentence. The appellant had pleaded guilty to one count of procuring another person to acquire financial products while possessing inside information contrary to Sections 1043A(1)(d) and 1311(1) of the Corporations Act 2001 (Cth) and one count of entering into an agreement to commit an offence under Sections 1043A(1)(d) and 1311(1) of the Corporations Act 2001 (Cth). The appellant had been sentenced to an overall term of imprisonment of eight years three months with a non-parole period of five years six months.

The appellant was the managing director of Hanlong Mining Investment Pty Ltd, a subsidiary of the Chinese corporation, Sichuan Hanlong Group Co Ltd. The appellant’s role was to identify possible opportunities for investment. In 2010, Bannerman Resources Ltd and Sundance Resources Ltd were identified as investment targets. In early 2011, the appellant was involved in the preparation of a potential takeover of both companies. In July 2011, Sichuan Hanlong decided to make takeover offers. Because of his involvement with Sichuan Hanlong, the appellant was aware of the decision shortly after it was made.

The appellant used his wife’s trading account and the trading company he owned and controlled to purchase financial products in both Bannerman and Sundance prior to the

announcement of the takeover. There was an agreement made with a Mr Zhu and others, whereby Mr Zhu would purchase financial products in Bannerman and Sundance for the benefit of the appellant and others using funds borrowed from Hanlong Mining.

The Court of Criminal Appeal had quashed the original sentence and imposed an overall term of imprisonment of seven years with a non-parole period of four years six months because of parity concerns, and because of the possibility that the sentencing judge erred in not taking account of evidence that the appellant would experience more onerous custody as he was a foreign national.

Notably, no error was established in respect of the sentencing judge’s findings that the conduct was ‘carefully planned and premeditated’, that the appellant’s attempts to conceal his involvement in procuring illegal trades was an aggravating feature of the offending, or by having multiple regard to the appellant’s concealment of his identity by making purchases that were not in his own name, or to the fact that the loan to finance the purchases was drawn from a related party of Hanlong Mining.

In *R v. Issakidis* [2018] NSWSC 378, the defendant was found guilty on 13 June 2017 by a jury, of two conspiracy offences, one contrary to Section 135.4(5) of the Criminal Code and one contrary to Sections 11.5(1) and 400.3(1) of the Criminal Code. The defendant and his co-conspirator were directors of Neumedix Health Australasia Pty Ltd. The defendant and his co-conspirator agreed to cause Neumedix Health to make false depreciation claims in its tax returns of many hundreds of millions of dollars. The depreciation claims were in respect of the alleged cost of acquisition by Neumedix Health of certain medical technologies, even though it was agreed that no such cost was to be incurred. This enabled Neumedix Health to avoid incurring tax liabilities on income it was deemed to have received as the owner of units in a number of trusts. These trusts generated very large taxable profits.

The defendant and his co-conspirator agreed to deal with the ‘proceeds of crime’, that is, to say amounts in various bank accounts that represented the cash distributions from the trusts to Neumedix Health. It was agreed that the funds be distributed offshore to various accounts controlled by entities associated with the defendant and then repatriated to Australia, largely for the benefit of the defendant and his co-conspirator.

Ultimately, an aggregate sentence of 10 years three months was imposed with a non-parole period of seven years six months, the sentencing judge determining that the offending was motivated by greed and that there was a strong need for deterrence as the offences were in the worst category (the loss to the Commonwealth was in excess of A$100 million).

In the case of *ACCC v. Yazaki Corporation* [2018] FCAFC 73, it was found that Yazaki Corporation had engaged in collusive conduct with a competitor, Sumitomo Electric Industries Ltd, in the course of supplying Toyota Australia with goods in the form of wire harnesses for motor vehicles. The offending cartel conduct involved an agreement, observed over an extended period, relating to requests for quotations issued by Toyota. Following the ACCC’s successful appeal against the fine imposed at first instance, the Full Federal Court of Australia imposed a penalty of A$45 million. This represents the highest financial penalty imposed under the Competition and Consumer Act 2010 (Cth).

These cases demonstrate an increased appetite on the part of the ACCC to commence proceedings against companies operating in Australia in relation to cartel conduct, as well as a trend of increasing financial penalties imposed by the courts in response to such conduct.

On 28 November 2018, following the lifting of long-standing suppression orders, previously restricted sentence proceedings relating to foreign bribery prosecutions against
Note Printing Australia Limited (NPA) and Securency International Pty Ltd (Securency) were released. On the facts as agreed in *The Queen v. Note Printing Australia Limited & Anor* [2012] VSC 302, both companies were subsidiaries for the Reserve Bank of Australia and were involved in the manufacture and supply of polymer banknotes used in Australia and internationally. The core offending conduct involved the payment of Indonesian, Malaysian, Vietnamese and Nepalese agents, engaged by the companies to assist in obtaining contracts with banks in the aforementioned countries.

While the substantial commission paid to overseas agents did not represent an offence, significantly it was demonstrated that Securency and NPA employees, including persons acting in the roles of general manager and chief financial officer, were aware that the local agents were paying a portion of their commission to bank officials with the intention of improperly influencing them in the exercise of their duties. These payments were described by Securency and NPA employees as ‘special commission’. Both companies were fined A$480,000, reduced by virtue of an undertaking on the part of both companies to provide future assistance to authorities.

In the case of *Australian Securities and Investments Commission v. Vocation Limited (In Liquidation) (No 2)* [2019] FCA 1783, the federal court delivered judgment on civil penalty proceedings against Vocation Limited and three of its officers who held previous roles as CEO, Chairman and CFO. The proceedings arose following an ASIC investigation into Vocation's entry into a Deed of Settlement with the Victorian Department of Education and Early Childhood Development in October 2014. All three officers where ultimately declared to have failed to meet the requisite standard of care and diligence in exercising company functions, in contravention of Section 180 of the Corporations Act 2001 (Cth.), following misleading representations made in relation to the company’s securities as well as failures to notify the Australian Securities Exchange (ASX) of relevant information. The company was also found guilty of providing the ASX with a defective cleaning notice, which was then relied upon to raise in excess of A$72 million from investors.

For failing to prevent misleading market disclosures, personal pecuniary penalties ranging from A$25,000 to A$70,000 were imposed against the three individuals and disqualification orders were made against each officer ranging from two to six years. A cost order was also made in favour of ASIC following the completion of proceedings.

On 11 March 2020, in *Australian Securities Investments Commission v. King & Anor* [2020] HCA 4 the High Court unanimously allowed an appeal from the Queensland Court of Criminal Appeal brought by ASIC and concerning the correct construction of Section 9 of the Corporations Act 2001 (Cth).

ASIC had initially brought proceedings against Mr King, the CEO and executive director of MFS Ltd, the parent company of a group providing funds management and financial services, alleging that Mr King had breached his duties as an ‘officer’ under Section 601FD of the Corporations Act 2001 (Cth). Significantly, the alleged breach related to activity of a subsidiary investment entity, MFS Investments Pty Ltd, at a time at which Mr King had ceased to be a director. The breach involved the unauthorised payment of company debts using a loan drawn down from the Royal Bank of Scotland.

The Queensland Court of Appeal found that Mr King did not fall within the capacity of an officer as he did not occupy a recognised position to which duties attached. By grant of special leave, ASIC appealed and the High Court found that the Mr King had the capacity to significantly affect the financial standing of the company and as such, should be deemed an ‘officer’ for the purposes of Section 9. As point of practice flowing from the decision, it
must be recognised that all persons who make decisions that effect subsidiary companies can potentially be held liable for the criminal or civil misconduct of the subsidiary, even when the such persons do not formally hold an office or position in the subsidiary.

As new legislation is introduced with increased maximum penalties, it is likely that the courts will approach sentencing principles such as general and specific deterrence against the new maximum penalties that will apply. This is likely to lead to an overall increase in the length of terms of imprisonment that will be imposed as punishment for serious white-collar offences.

VI CONCLUSIONS AND OUTLOOK

It is anticipated that the next 12 to 18 months will be a period of increased legislative and policy reform in the area of white-collar crime. Central to this reform are the final recommendations of the ALRC in relation to corporate criminal responsibility, which have the potential to prompt radical legislative transformation of Australia’s existing criminal liability regime for corporate bodies.

The forecasted changes include the new anti-money laundering and counter-terrorism financing laws that have been implemented by the AUSTRAC. These laws regulate digital currency exchange (DCE) providers operating in Australia. Businesses that are operating in Australia must register with the AUSTRAC and meet the Australian government’s anti-money laundering and counter-terrorism compliance and reporting obligations. The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) requires regulated entities to collect information to establish a customer’s identity, monitor transactional activity, and report to the AUSTRAC any transactions or activities that are suspicious or involve large amounts of cash (over A$10,000). It is foreseeable that regulatory investigations into DCE compliance with Australia’s anti-money laundering legislation will be on the regulators’ agenda in the next 12 months.

It is also expected that amendments will be made to certain penalty provisions of the Criminal Code to bring it in line with the Senate Economics References Committee March 2017 report, ‘Lifting the fear and suppressing the greed: Penalties for white-collar crime and corporate and financial misconduct in Australia’. The report recommended an increase in civil penalties under the Corporations Act 2001 (Cth) for individuals and companies, a change in the manner in which civil penalties are calculated and empowering the ASIC to have disgorgement powers. Following the commencement of the Treasury Laws Amendment (Strengthen Corporate and Financial Sector Penalties) Bill 2018, a number of these proposed changes are presently in force.
I INTRODUCTION

A distinction has to be made between the police and judicial authorities in Austria with respect to law enforcement authorities. In general, the police as the law enforcement authority, who are subordinate to the respective public prosecutor, lead the investigation. The public prosecutor is the head of investigations and responsible for the prosecution of crimes. A permit regarding investigations is in general not required; for example, to question witnesses. However, specific permission from the court is necessary if the public prosecutor decides to take special investigation measures, such as house searches (raids), opening of accounts or telephone tapping. All investigation measures are usually carried out by the police. Regarding the powers of the prosecution authorities, there is no distinction between corporate criminal proceedings and the prosecution of individuals.

After the investigation procedure has been completed, the public prosecutor decides, based on the results of the investigation, whether to press charges against the defendant (either an accused individual or a corporation) or whether proceedings should be discontinued.

The Central Public Prosecution for the Enforcement of Business Crimes and Corruption (WKStA) is a special prosecution authority that was established in 2011 as a response to the increasing number and complexity of white-collar crimes. It is in charge of prosecuting all Austrian business property crimes involving sums exceeding a certain amount or involving serious cases of corruption.

A special feature of Austrian criminal law is the reporting obligations of the public prosecutors. The public prosecutor must report crimes to its superior public prosecutor’s office if there is an overriding public interest resulting from the significance of the crime or the suspect. If the importance of the crime is not restricted to the locality, the High Public Prosecutor’s Office has to submit another report illustrating the premeditated procedural actions to the Federal Ministry of Justice. Thus, the reporting chain can range from the investigating or prosecuting public prosecutor to the Federal Ministry of Justice. Corresponding to the obligation of public prosecutors to report to higher authorities, these higher authorities have the right to issue instructions to subordinate public prosecutors.

The possibility of directives being given by higher public prosecutors has been the subject of numerous discussions, since critics stated that the prosecution should be – as part of the jurisdiction – as independent as courts and, therefore, directives given by higher public prosecutors would be improper. Therefore, a commission of experts was set up in 2014 to make a proposal concerning each single case that is reported to the Minister.

1 Norbert Wess and Vanessa McAllister are partners and Markus Machan is attorney at wkk law Rechtsanwälte.
Since the Austrian Code of Corporate Criminal Liability (VbVG) came into effect on 1 January 2006, companies and other legal entities can also be accused in criminal proceedings and, like natural persons, can be (under given circumstances) held liable and be convicted. Depending on the conduct of the legal entity following the crime, the prosecutor is entitled to refrain from prosecuting if the prosecution seems unnecessary. Comprehensive cooperation with the prosecution and the installation (or adjustment) of an efficient surveillance system (for the future) can, in fact, protect the legal entity from further prosecution, but not the accused individual.

II CONDUCT

i Self-reporting

In terms of corporate and business crimes, Austrian law does not provide for a specific regulation governing self-disclosure that would exempt the perpetrators from punishment. However, if an offender or a legal entity that has committed or is responsible for a crime shows active repentance, the punishment may be exempted. What is expected from the individual or legal entity when showing repentance after committing an offence is precisely specified by law. The offender or the legal entity has to be willing to remedy the damage voluntarily even if only pressed by the victim, or at least commit himself or herself to compensating the damage without the law enforcement authorities becoming aware of the offender's guilt.

Self-disclosure is a special and very important feature in Austrian tax law. Taxpayers can often be exempted from quite substantial punishment by self-disclosure. The tax enforcement authorities, in turn, do not have to lead (lengthy) investigation procedures; however, self-disclosure only exempts offenders from punishment under circumstances that are strictly specified by law and that have been considerably tightened over the years.2

In financial criminal law, an exemption of punishment is only possible by means of self-disclosure if it occurs before an offence has been discovered or before the first prosecution measures against the self-disclosing person or business have been taken. In the case of an ongoing audit, self-disclosure has to take place when the audit starts. Owing to a recent modification, a tax surcharge is added when the offender is guilty of an intentional or grossly negligent tax offence.

In addition, within the scope of self-disclosure, the misconduct and all relevant circumstances that are important in determining the evaded amount or the tax loss have to be disclosed. If the self-disclosure is inaccurate to the extent that not all the relevant facts are disclosed, tax evaders will not be exempt from punishment. Moreover, the amount due must be paid within a month. It is possible, however, to apply for payment in instalments over a maximum of two years.

Austrian competition law3 also provides for a legal remedy with an effect similar to self-disclosure. The Federal Competition Authority (BWB) may refrain from requesting a fine in the event of violation of cartel regulations if a corporation that has violated cartel regulations is the first to disclose information and evidence to the BWB that allows it to file a well-founded request permission to carry out a house search. If the corporation is not the

---


3 Competition law is technically regulated outside criminal law; however, the cartel fine is a criminal penalty in the meaning of Article 6 ECHR; see McAllister, Die Kartellgeldbuße (2017) 83.
first to provide new information, it still can benefit from this regulation if the information disclosed allows the BWB directly to file an application (to the Cartel Court) to impose a fine.

Furthermore, it is required that the corporation has ceased violating cartel regulations and that it fully cooperates with the BWB in investigating the facts. The corporation must also not have forced any other business to participate in the violation of cartel regulations. If the corporation does not fulfil the requirement of being the first (whether to enable a house search or an application to impose a fine), but it complies with all the other aforementioned conditions, the cooperation may lead to a reduced fine.

Complementary to this legal remedy in competition law, the Code of Criminal Procedure contains a leniency programme applicable to offences perpetrated by employees or executives (e.g., Article 168b Criminal Code – collusive bidding) if the corporation benefits from the leniency programme provided by competition law. Furthermore, a general leniency programme (adapted via an amendment in 2016) enables an ‘alternative reaction’ in the meaning of ‘out-of-court offence resolution’ basically limited to small offences. If such an alternative reaction is not possible in particular cases (e.g., the offender did not comply with all the requirements), the offender can at least benefit from an ‘extraordinary mitigation of punishment’.

ii Internal investigations

Internal investigations into corporations are increasingly gaining importance in Austria. The purpose of internal investigations is to gain a full and detailed picture of any criminal or illegal conduct of employees and executives if unlawful conduct in the corporation has occurred or is suspected. The results of internal investigations may also be made available to the public prosecutor, who may be investigating simultaneously, or to the interested public (e.g., concerning stock market-listed corporations).

Regarding sophisticated cases, there is often a requirement to set up an entire internal investigation team consisting of specialists within the corporation, optionally supported and strengthened by external experts, such as auditors and specialised attorneys at law. This team is in charge of seizing, preparing and analysing relevant data within the scope of the investigation. After screening the data, it may also be necessary to question former or current employees of the corporation about any incidents. During such ‘forensic interviews’, the interrogated person may (very often) incriminate himself or herself by a statement, hence an interview can be conducted only if the person cooperates voluntarily and is given the opportunity to consult an attorney at law in advance.4

There is no obligation to share the results of an internal investigation with law enforcement authorities, but if the corporation decides to cooperate with the enforcement authorities, there may be conflicts of interest with the company’s current or former employees. This must be pointed out by the legal counsellor from the outset.

---

4 See Wess, ‘Unternehmensinterne Ermittlungen – Erfahrungen und Problemstellungen in Österreich’, Anwaltsblatt, 2013, 223. There is an ongoing discussion whether an employee has to disclose all his or her knowledge (owing to the employee’s duty of good faith) even if it may result in self-incrimination; see, for example, Zerbes, ‘Strafrechtliche Grundsatzfragen “interner Untersuchungen”’, in Lewisch (ed.), Wirtschaftsstrafrecht und Organverantwortlichkeit Jahrbuch 2013 (2013) 271.
A few years ago, there was a discussion\(^5\) regarding whether law enforcers are entitled to request the surrender or to effect the detention of documents and reports kept by the corporation against its will. As a result of an amendment to the Code of Criminal Procedure in 2016, the correspondence with an attorney concerning, for example, an internal investigation is also protected if it is in the company's custody (and not only in the lawyer's office). These documents (even in the company's custody) cannot be confiscated; illegally obtained documents containing correspondence with a lawyer are subsequently inadmissible in court.

iii Whistle-blowers

Internationally, many corporations and public institutions already rely on whistle-blowers in the prevention of business crimes and corruption. There is no obligation for corporations in Austria to make anonymous whistle-blowing facilities available; however, the establishment of whistle-blowing facilities is increasingly acknowledged as part of modern risk management. Appropriate whistle-blowing facilities can consist of a corporation's own hotline, an email address established specifically for this purpose or a suitable internet platform. Often the corporation mandates a third party (e.g., a law firm) with execution of the hotline. The offences reported to these whistle-blowing facilities are not necessarily limited to internal offences against criminal law within the corporation; violations of labour law and environmental regulations may also be the subject of whistle-blowing reports.

In general, whistle-blowing facilities create certain tensions between an employee's duty of loyalty as defined by labour law (which goes beyond the general duty to work) and the employer's duty to have regard for the welfare of employees. Thus, the employee's duty of loyalty, according to which the employee has to safeguard the operational interests of the employer in the course of his or her work, may oblige the employee to report violations of regulations by other employees of which he or she has become aware. An obligation to spy on other employees can usually not be assumed. Regarding certain employees, however (e.g., employees of internal review or control departments), an extended obligation to report may already result explicitly from the agreed work activity.

If an employee aims to conceal serious violations of rules by other employees, he or she may prove to be undeserving of the employer's confidence. This can also result in a subsequent (summary) dismissal. Owing to the fact that an employer is obliged to have regard for the welfare of his or her employees, it would, however, not be appropriate to monitor an employee based on unsubstantiated and unfounded reports to document any further violations of rules.\(^6\)

Certain legal provisions may encourage or even force an employee to notify the authorities or a compromised corporation of unlawful conduct. For example, persons trading financial instruments in their profession are obliged to notify the Financial Market Authority without delay when there is reason to suspect that a certain transaction could represent insider trading or market manipulation.

Depending on its precise design, an established whistle-blowing facility may be a monitoring measure or system that could potentially affect human dignity. For this reason,


\(^{6}\) See ECHR 9 January 2018, 1874/13, López Ribalda and others / Spain (video surveillance due to suspicion of theft by employees).
the introduction of a whistle-blowing facility requires the prior consent of the workers’ council. If there is no workers’ council, the consent of each employee has to be obtained in advance.

When implementing a whistle-blowing facility, data protection regulations have to be taken into consideration. The data inspection board dealing with whistle-blowing facilities must evaluate whether appropriate safeguards have been taken to prevent unauthorised access to collected data.

Moreover, the Austrian judicial authorities have established their own whistle-blowing home page. It is an anonymous interactive platform that is specifically maintained by the WKStA. Instead of being a mere reporting system that allows users to submit a message with a specific suspicion, this platform also offers the possibility of a mutual communication between the informant and the authorities, in which the informant (if desired) can remain anonymous.

This institution was set up in March 2013 and has been frequently used since then. In the first complete year of its existence (2014), more than 1,900 tip-offs had been registered, only 6 per cent of which were dismissed as being unsubstantiated. However, in the following years, there have been – including 2018 – consistently about 1,000 tips per year. Although only about 7 per cent of the tips cause themselves the initiation of criminal proceedings, many of these tips are being used as further evidence in already on-going investigations. All in all, information obtained from this platform has already led to a number of charges and convictions, thus proving its effectiveness.

### III ENFORCEMENT

#### i Corporate liability

The VbVG is a separate law that regulates the criminal liability of corporations organised as legal entities (see Section I). The criminal liability of a corporate entity results from criminal offences committed by its employees or decision makers. Irrespective of the level of seniority of the individual offender, liability of a corporate entity is only given if the offence was committed in favour of the corporate entity or if obligations relating to the corporate entity were infringed. An offence is already regarded as being to the benefit of a corporate entity if it has improved its competitive situation; material gain is not required. Obligations of the corporate entity that, if violated, may result in its liability, can be related to all areas of law.

Regarding offences of a decision maker, the corporation is (criminally) liable if the decision maker has committed the offence unlawfully and culpably. Decision makers are, as the VbVG states, above all, persons who are authorised to represent a corporate entity externally, such as members of the board of directors or managing directors.

The statutory prerequisites for holding a corporate entity liable as a result of the criminal offence of a (non-executive) employee are more comprehensive. The criminal offence committed by the employee must have been made possible or substantially facilitated by the corporation’s failing to take measures in terms of technology, organisation and personnel to prevent such an offence. The employee must not have acted culpably (e.g., he or she can be exculpated owing to a mistake of law).

---

As described above, the criminal liability of a corporate entity depends solely on the criminal relevance of acts of its employees or decision makers. As specified, this may lead to serious conflicts of interest between prosecuted individuals and the corporate entity. For this reason, attorneys at law are advised against representing corporate entities and prosecuted individuals in the same case as this could cause a conflict with respect to the professional prohibition of dual representation.

ii Penalties

Corporate entities that are liable for criminal offences are punished only with fines. The amount of the fine is determined by the number of ‘daily rates’ imposed and the amount of the daily rate. The range of punishment (number of daily rates for the offence in question) depends on the seriousness of the offence committed and is derived from the penalty range applicable for individuals (e.g., an offence punished with 10 to 20 years or life imprisonment may lead to a fine with up to 180 daily rates imposed against the corporate entity). The next step is for aggravating and mitigating circumstances to be taken into consideration, to determine the specific number of daily rates within this range (e.g., if the maximum is 180 daily rates, the court might find 60 daily rates adequate in the specific case). An aggravating circumstance can be the amount of damage caused by the criminal offence as well as the level of unlawful conduct by employees that was tolerated or even promoted. Mitigating circumstances include whether the corporate entity participates in uncovering the infraction, remedies the consequences of the offence or takes precautions to prevent such offences in the future. In practice, the maximum number of daily rates for business crimes that are relevant is 130.

The amount of an individual daily rate results from the corporation’s profitability, taking into account the corporation’s economic performance. A daily rate corresponds to 1/360 of the corporation’s annual yield (this amount may be exceed or fall below by a third). The maximum amount of a daily rate, irrespective of the corporation’s economic performance, is €10,000.

iii Compliance programmes

The establishment of a compliance programme does not automatically release a corporate entity from its criminal liability. The VbVG explicitly regulates that preventive measures (one example being an established compliance programme) taken both before and after the offence are considered mitigating circumstances. If the corporate entity involved has already taken preventive measures before the offence – which later, however, turn out to be inappropriate – and if, consequently, efforts to prevent such violations of laws by employees are obvious, this will (at least) lead to a significant reduction of the penalty. The same holds true for a corporate entity that decides – following the disclosure of misconduct by employees or decision makers – to establish a compliance programme or to remedy its weaknesses to avoid future misconduct.

The implementation of suitable training programmes or the drafting of guidelines for employees in sensitive fields of work are other examples of preventive compliance programmes seen as mitigating circumstances. In addition, the promotion or establishment of a whistle-blowing system may be regarded as an important step to prevent similar offences in the future.

An essential contribution to uncovering a crime may also lead to a reduction of the fine imposed on the corporate entity. That contribution will be realised more easily if a
Austria

compliance programme with comprehensive duties of documentation or support for the corporation’s internal review is already in place. These documents will most likely facilitate a review of the decision-making process in retrospect.

Furthermore, a reduction of the fine in the event of a criminal conviction can be achieved with the argument of impeccable business conduct. This mitigating circumstance for legal entities (liable under VbVG) corresponds with that of ‘proper moral conduct’ of natural persons. Impeccable business conduct is certainly indicated and supported by the establishment of a comprehensive and, above all, effective compliance programme.

In addition to many other advantages, the purpose of a compliance programme is, by definition, to prevent the commission of criminal offences in business. If a compliance programme has been successfully established and integrated into the corporate culture, this may well mean that the corporate entity should be able to produce evidence of its impeccable business conduct if convicted (for the first time). An effective compliance system can help a corporate entity that has already been liable once for an offence to show good conduct over a longer period.

iv Prosecution of individuals

Regarding the criminal liability of individuals in connection with the criminal liability of companies, it has to be taken into account that the criminal liability of companies always depends on the unlawful conduct of individuals (employees or decision makers). Only in exceptional cases, the employee who triggered the criminal liability of the company would go unpunished (e.g., if he or she did not act in a ‘culpable’ manner).

If an investigation against individuals working in the company is launched, the fundamental question for the company is whether it intends to cooperate with the defendants’ counsel. In the event of close cooperation with the defendant, it is likely that criminal charges will be brought against the individual and also (after further analysis) against the company. In this respect, the invalidation of accusations against the individual can subsequently weaken the accusation brought against the company. Ultimately, it is at the discretion of the company to choose to cooperate with the defendants.

As the dismissal of employees or decision makers being criminally charged cannot always hinder the imposition of a fine against a company, the company – in cooperation with specialised attorneys at law – should devise a strategy for dealing with these individuals. At the same time, law enforcement authorities must be convinced (i.e., by the company cooperating as closely as possible) to refrain from bringing criminal charges against the company.

IV INTERNATIONAL

i Extraterritorial jurisdiction

In general, Austrian criminal law applies to all offences committed in Austria. This corresponds to the principle of territoriality that is now common practice for the application of statutes. Regardless of the foregoing, Austrian criminal law also applies to certain offences explicitly specified by law even if they were committed abroad.

The legal provision that crimes of corruption and bribery will be prosecuted in Austria, regardless of where the crime was committed if only the offender is Austrian, is of particular relevance for companies. These crimes are also prosecuted in Austria if the offence was committed to the benefit of an Austrian public officer.

© 2020 Law Business Research Ltd
If an Austrian citizen as an employee or decision maker of a company bribes a foreign public officer, he or she has to be punished pursuant to Austrian criminal law. This applies regardless of whether the crime was committed in Austria or abroad and whether it was an Austrian or foreign company. Conversely, decision makers or employees of foreign companies can be held criminally liable in Austria if they bribe an Austrian public officer – even from another country.

This type of special regulation goes far beyond the original principle of territoriality. In reality this means that bribery committed anywhere in the world by Austrian citizens or of Austrian public officers can be prosecuted in Austria.

### International cooperation

The Austrian criminal justice authorities cooperate closely with those in foreign countries. The applicable legal basis is laid down in bilateral or multilateral international treaties and their respective implementation in Austrian law.

The Austrian Administrative and Judicial Assistance Act regulates, for example, the circumstances under which an extradition request to foreign criminal justice authorities can take place. This Act also contains several provisions governing general judicial assistance, and the takeover of criminal prosecutions, as well as the takeover of surveillance by Austrian authorities. The statutes specify reciprocity as a general prerequisite for these measures. In addition, administrative and judicial assistance requests must not infringe on public policy or the national interests of Austria.

Austria does not extradite individuals who commit petty crimes. Extraditions from Austria are only admissible in the case of intentional offences and for those who carry a prison sentence of more than one year pursuant to foreign and Austrian law. Austria does not, however, extradite to countries in which criminal proceedings are not in compliance with the fundamental principles of the European Convention on Human Rights (ECHR), or if the person extradited is at risk of political persecution, suffering cruel or humiliating punishments, or even the death penalty. In principle, Austria does not extradite its own citizens. However, there is an exemption with respect to extraditions to the International Criminal Court.

The influence of European Union (EU) law on the criminal law of individual Member States is becoming more important in practice. European law can specify, for example, minimum requirements for the determination of offences and penalties and for the facilitation of the mutual recognition of court sentences and decisions.

Extraditions to EU Member States have been specifically regulated by an EU Directive that was implemented in Austria by federal law with respect to judicial cooperation in criminal cases with EU Member States. This encompasses both pending foreign criminal proceedings (extradition for pretrial detention) and non-appealable sentences (execution of a sentence). These processes have been substantially simplified, compared with extraditions to third countries, owing to the principle of mutual recognition of criminal sentences passed by European states. It is also required that human rights standards are observed across Europe. For a number of specified offences, the requirement of reciprocity, for example, is no longer a prerequisite for extradition to another EU Member State. Consequently, a person who is prosecuted by an enforcement authority can also be extradited for an offence that is not punishable in Austria.

© 2020 Law Business Research Ltd
iii Local law considerations

In cross-border cases that have an impact on Austria, some special features have to be taken into consideration in criminal investigations. Austria still has banking secrecy laws that are comparatively strict. Information concerning transactions may only be given with prior approval of the court based on a motion filed by the public prosecutor. However, banks now have to report current accounts, building society accounts, passbooks and securities accounts to a central account register. Since 2017, Austria also participates in the international exchange of information on bank accounts.

There is also a strict obligation of secrecy regarding certain professional groups, such as attorneys at law, auditors and tax consultants. This obligation may not be invalidated by the seizure or confiscation of communications. Thus, members of these professional groups have the right to object to seizure. In the event of an objection, a court has to decide whether the seized communications are covered by professional secrecy. These communications may not be exploited by law enforcement authorities before the court has decided that the seized communications are not protected by the relevant professional secrecy.8 The protection of other professional groups, such as banks, has substantially softened in recent years. Therefore, it is now much easier for law enforcement authorities to gain access to communications from banks.

V YEAR IN REVIEW

In 2020, there have been several changes in the Austrian Criminal Procedure Law in response to the worldwide covid-19 pandemic. These changes are mostly limited to the duration of the protective measures against the coronavirus. They especially include a suspension of legal and judicial deadlines (e.g., for filing an appeal against a judicial decision) or the possibility to question a suspect who is held in pretrial detention via a video conference.

Apart from these changes connected to the covid-19 pandemic, the following amendments in the Austrian Criminal Law in the last year are worth mentioning.

In 2019, the Violence Protection Act 2019 entered into force, which – with regard to the criminal law aspects of this legislative package – aims to strengthen the procedural rights of the victims, especially victims of domestic violence and of sexual crimes.

Another update of the Austrian Criminal Law concerns the implementation of the Directive (EU) 2017/1371 on the fight against fraud to the EU’s financial interests by means of criminal law. Since 28 December 2019, there are two new criminal offences described in the Austrian Criminal Code: Article 168c and Article 168d punish fraudulent acts affecting the revenue or expenditure and the assets of the EU budget.

An ‘Adaption Act’ in 2020 aimed to adjust the Austrian Criminal Law to European legislation in specific areas (e.g., with regard to extradition proceedings, juvenile criminal cases and the cooperation with international courts such as the International Criminal Court). This amendment also strengthened the right of suspects to contact a defence counsel on standby as soon as he or she has been arrested and it clarified that, if the prerequisites are met, a public defender has to be appointed without delay.

Finally, one legislative change within the Austrian Criminal Procedure Law has not been made by the legislative bodies, but was caused by a decision of the Austrian Constitutional Court. On 11 December 2019, the Constitutional Court ruled that Articles 134 (3a) and 135a Austrian Criminal Procedure Code contradict the constitution and it therefore repealed these two provisions (along with provisions outside of Criminal Law). The Austrian Constitutional Court stated that Articles 134 (3a) and 135a – that gave the public prosecutor the power to covertly monitor encrypted messages by installing a program on a computer system – conflict the right to privacy according to Article 8 ECHR, which has in Austria constitutional status. The court also found that the proportionality of the measures was not observed. The decision of the Constitutional Court was taken following two appeals lodged by several members of the Austrian Parliament. Because the decision of the repeal was announced even before Articles 134(3a) and 135a have entered into force (which would have been in April 2020), these provisions have never actually been applied.

VI CONCLUSIONS AND OUTLOOK

The accomplished amendments mainly address individual procedural rights of suspects and victims in criminal proceedings and aimed at implementing several Directives of the European Union. Clearly, many legislative changes in Austrian Criminal Law that have been made in the first months of 2020 are part of necessary measures to prevent the spread of the coronavirus. Although most of them are limited to the duration of the worldwide covid-19 pandemic, it remains to be seen what long-term consequences the pandemic will have for Austrian Criminal Law.

I INTRODUCTION

Both at the EU level and in the Member States (including Belgium), a wide variety of authorities and regulators are empowered to supervise, investigate and sanction corporate conduct. Each of these has various and often very intrusive powers; for example, to carry out unannounced inspections and house searches, to seize documents, to trace telecommunications, to access IT systems and to interrogate persons.

Besides the traditional criminal authorities, there are numerous regulators that, albeit strictly speaking active in the regulatory and administrative field, have far-reaching investigative and sanctioning powers as well. These powers often do not differ significantly from the powers of criminal authorities. Because of the nature and effects of the measures taken and sanctions imposed by these regulators on the corporates and individuals (e.g., senior managers) affected by them, these persons often benefit from the same fundamental rights and guarantees under European Union (EU) and national law that apply to purely criminal sanctions.

Well-known examples of regulatory authorities are, at both the EU and national level, the competition authorities (which wield powers across all sectors and areas of economic activity), the financial and banking regulators (which supervise, investigate and sanction the conduct and activities of financial services providers, including banks), and, more recently, the data protection authorities (which investigate and sanction breaches of data protection rules and raise awareness in this respect).

In what follows, particular attention is paid to the powers of competition and financial regulators. This is not to underestimate the role and powers of an increasing number of other regulators of all types, which corporates especially need to take into account. For instance, the Economic Inspectorate (a body attached to the Belgian Federal Public Service of Economy) has powers in areas that concern trade practices and consumer protection, and that will also apply to the conduct and activities of financial institutions (e.g., in the framework of the marketing and distribution of financial instruments to the public). The same applies to tax, labour and environmental authorities, to name just a few. While their prerogatives and powers might often appear to be similar, it remains nonetheless important, for persons affected by them, to properly assess the following:

a which specific statutory and legislative rules govern the scope of their mandate and competences; and

b the precise nature and impact of their powers. This assessment ensures that:

---

1 Stefaan Loosveld is a partner and Sarah Benzidi is an associate at Linklaters.
the actions and measures taken by these regulators remain within the confines of what they are legally entitled to do; and

• these regulators comply with the fundamental rights granted to those affected by these actions and measures. A transgression of these confines or a lack of compliance with this protection renders their actions and measures unlawful.

II CONDUCT

i Self-reporting

As a general principle, a person is not obliged to incriminate himself or herself.² Hence, no duty exists for a party to report its own criminal offences. However, one may choose to report an offence voluntarily to obtain leniency or a settlement (see below). Nor is there a general duty to report criminal offences committed by third parties, with the exception of crimes against public safety or against the life or property of an individual. The latter category of crimes should be reported to the public prosecutor. Failure to do so is criminally sanctioned.

Similarly, a person who is the subject of a regulatory investigation that can lead to the imposition of a financial penalty or fine has a right to silence and a right not to self-incriminate. The regulators have already acknowledged these rights in the context of replying to the written questions asked in the framework of a regulatory investigation. The same right applies in case of an interrogation.

These rights may also be violated if the regulator uses constraints to obtain evidence. A constraint may be to impose a penalty or fine if the entity concerned fails to hand over evidence that the regulator requests. However, constraints may be lawful if their aim is to obtain evidence that exists independently of the will of the entity concerned. In addition, the right to silence cannot be invoked to prevent handing over documents to the regulators if the entity concerned has a statutory duty to keep the documents as records.

Belgian regulators have no duty to caution (i.e., to inform the entity under investigation at the beginning of the interrogation about its right to silence), but as a result of case law, when the regulators remind an undertaking of its right to silence, it prevents any future objection relating to the right not to self-incriminate.

The right not to self-incriminate can normally only be invoked by a person who is facing a criminal charge within the meaning of Article 6 of the European Convention on Human Rights (i.e., when that person can legitimately infer from his or her situation that he or she is suspected of having committed certain offences and that proceedings are likely to be brought against him or her). This means that a request based on this right by an undertaking that the regulator does not use some of the documents that the undertaking previously provided to the regulator will rarely be granted, especially if the undertaking submitted such documents before facing a criminal charge.

Leniency in competition law matters

Undertakings are not obliged to self-report when they discover an internal wrongdoing that could constitute a competition law infringement. They may, however, voluntarily opt to do so in competition cases to benefit from the leniency programme.

Under EU competition law, the conditions and benefits of leniency applications are enumerated in the Commission Notice on Immunity from fines and reduction of fines in cartel cases (Commission Leniency Notice). Undertakings that are part of a cartel can apply for leniency. By contrast, abuses of dominant position, vertical agreements and horizontal agreements that are not cartels within the meaning of the Commission Leniency Notice cannot benefit from the leniency programme.

Leniency is granted on a first-come, first-served basis. If an undertaking or association of undertakings wants to obtain full immunity from fines, it must be the first to submit information and evidence enabling the European Commission to carry out a targeted inspection or to establish an infringement. A company that does not qualify for full immunity can apply for a reduction of the fine if it provides evidence that represents significant added value to the evidence already in the possession of the European Commission.

In all cases, the leniency applicant must also end its involvement in the alleged cartel (except when the European Commission decides otherwise to preserve the integrity of inspections), cooperate fully and expeditiously with the European Commission throughout its investigation, and provide all evidence in its possession. The applicant may not destroy, falsify or conceal any evidence relating to the alleged cartel, either prior to the submission of the application or during the investigation.

The regime of leniency under Belgian competition law follows closely the European regime. The rules regarding leniency are contained in Book IV of the Belgian Code of Economic Law and the Leniency Guidelines of 22 April 2016. Thus, an undertaking can apply at Belgian level for full or partial immunity of fines, provided it offers sufficient evidence, collaborates fully and ends its involvement in the cartel. However, a few notable differences exist with the EU system. First, leniency under Belgian competition law also applies to ‘hub-and-spoke’ conspiracies. Second, Belgian competition law provides for administrative sanctions for individuals involved in certain serious violations of competition law (in essence hardcore cartels). For these individuals, the Leniency Guidelines provide a regime of immunity of fines, for which the individuals can apply separately or with the undertakings employing them. If granted, the individuals will be fully immune.

In assessing whether the conditions for leniency are satisfied, both the European Commission and the Belgian Competition Authority (BCA) enjoy a margin of discretion. A company cannot be certain whether the competition authorities will consider the information provided to be sufficient to qualify for immunity or fine reduction. Also, leniency applications, both under European and Belgian competition law, provide no protection against private law claims for damages from customers or competitors.

3 Commission Notice on Immunity from fines and reduction of fines in cartel cases (OJ C 298, 8 December 2006, p. 17).
4 Guidelines on Leniency Notice on full or partial immunity from fines in cartel cases (Belgian Official State Gazette, 22 March 2016, p. 19796).
5 These are cartels involving both manufacturers and suppliers, whereby one side of the market acts as a ‘hub’ to facilitate coordination between players on the other side of the market.
Under the Antitrust Damages Directive, implemented in Belgian law, final decisions by the competition authorities (e.g., the BCA in Belgium) will constitute irrefutable proof of fault in private damage claims. The Antitrust Damages Directive also facilitates disclosure of evidence. However, leniency statements at both the EU and Belgian levels are shielded from requests for disclosure. Other documents in the investigation file may be disclosed, albeit that the court must balance the interests of the victims with the interest of effective public enforcement of competition law (i.e., keeping the leniency programme attractive for undertakings).

Before deciding to file a leniency application, companies should, therefore, make a careful assessment of all relevant elements, including the likelihood of an investigation or a fine, the risk of a leniency application by another cartel member, the potential impact of a leniency application on the risk of investigations in other countries, the risk of private damage claims from third parties, and the potential effect on relationships with other industry players and with customers.

**Internal investigations**

An undertaking may conduct its own internal investigations. There are several ways to do so, such as interviewing the relevant employees and auditing their paper and electronic files. An undertaking’s internal investigation must comply with rules regarding privacy and employee protection, arising from various provisions from employment, telecommunication and privacy law. Moreover, under Belgian law, former workers are not obliged to cooperate with internal investigations, unless their employee contracts include a post-employment cooperation obligation.

An undertaking will often need to conduct an internal investigation when preparing a leniency application (to provide full cooperation) or answer a request for information from the Competition Authority, the financial services regulators and banking supervisors, and criminal authorities. While certain legislation provides, under penalty of sanctions (e.g., fines) in the case of refusal, for an obligation on the undertaking to provide complete and correct information to the authorities, this obligation cannot trump the right for the undertaking concerned not to incriminate itself and to invoke this right by refusing to hand over certain documents. However, as soon as a document or a piece of information is voluntarily provided to the authorities, the undertaking cannot claim any attorney–client or other legal privilege on it.

Among other things, in competition law matters, Book IV of the Belgian Code of Economic Law now introduces administrative fines for individuals (as mentioned above, employees may now also apply for individual leniency in relation to hardcore infringements). In other areas (e.g., market abuse), certain conduct might even be criminally sanctioned. Employees might, therefore, seek the assistance of their own counsel in the event of an internal investigation by their employer.

---


7 On 6 June 2017, Belgium adopted legislation transposing the Antitrust Damages Directive. This legislation became applicable as of 22 June 2017.
iii Whistle-blowers


Until recently, there was no cross-sectoral EU legislation dealing with such mechanisms generally. This has changed with the adoption on 7 October 2019 of the Whistle-blowing Directive.8 EU Member States have until 17 December 2021 to implement the Directive into their national legislation.

This Directive lays down minimum standards for the protection of ‘reporting persons’ (i.e., individuals (natural persons) reporting or publicly disclosing information on breaches acquired in the context of their work-related activities) and ‘persons concerned’ (i.e., individuals or legal entities who are referred to in the report or public disclosure as persons to whom the breach is attributed or with which they are associated). The employment status of the reporting person, and whether or not that person works in the private or public sector, is irrelevant. The protection also applies to, for instance, shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including the non-executive members thereof.

The breaches relate to an extensive list of EU legislations in a variety of areas that go beyond financial services or anti-money laundering (AML). They also include, among others, public procurement, product safety, transport safety, protection of the environment, food safety and health, consumer protection, the protection of privacy and personal data, and IT-security. This Directive contains in this sense the ‘default rules’, whereas the rules on whistle-blowing that are contained in specific EU legislation will continue to apply.

The Directive first obliges EU Member States to ensure that legal entities set up internal reporting channels and procedures. As a rule, this obligation does not apply to legal entities in the private sector with less than 50 employees. As an exception, undertakings that are active in the financial sector or that are otherwise obliged entities for AML purposes are always captured by this obligation. Legal entities in the private sector with 50 to 249 employees are allowed to share resources for the receipt and possibly investigation of whistle-blowing reports.9

EU Member States are also obliged to establish external reporting channels and to designate to this effect the authorities competent to receive, give feedback and follow up on reports. As the Directive captures more areas than those for which there are currently already competent authorities in place for such external reporting, EU Member States will undoubtedly need to establish new authorities that are specifically competent for such reporting.

Besides internal and external reporting channels, the Directive also protects in certain circumstances ‘public disclosures’ (i.e., persons who publicly disclose information on breaches falling within the scope of the Directive).

9 The Directive provides for the possibility for EU Members to grant similar exemptions for legal entities in the public sector.
Finally, the Directive obliges EU Member States to provide for a wide range of protections for reporting persons and persons concerned. These cover, among others, the confidentiality of their identity (albeit with important exceptions), the compliant processing of their personal data and the protection against retaliation.

EU whistle-blowing legislation in the area of financial services

At the EU level, various legislation in the areas of financial services generally and banking specifically contain rules on the establishment of whistle-blowing mechanisms. These mechanisms also typically have an internal dimension (i.e., procedures for the reporting of possible infringements by employees to their employer) and an external dimension (i.e., procedures with the regulators for the reporting of possible infringements to the regulators by employees or other persons that deal with financial services firms or banks).

Thus, for instance, Article 32 of the EU Market Abuse Regulation\(^\text{10}\) requires Member States to ensure that the respective national administrative authority that is competent for market abuse infringements establishes effective mechanisms to enable reporting of actual or potential infringements of this Regulation. These mechanisms must include at least:

\(\textbf{a}\) specific procedures for the receipt of reports of infringements and their follow-up, including the establishment of secure communication channels for such reports;

\(\textbf{b}\) within their employment, appropriate protection for persons working under a contract of employment who report infringements or are accused of infringements, against retaliation, discrimination or other types of unfair treatment as a minimum; and

\(\textbf{c}\) protection of personal data both of the person who reports the infringement and the natural person who allegedly committed the infringement, including protection in relation to preserving the confidentiality of their identity, at all stages of the procedure without prejudice to disclosure of information being required by national law in the context of investigations or subsequent judicial proceedings.

The Market Abuse Regulation also obliges Member States to require employers who carry out regulated activities to have in place appropriate internal procedures for their employees to report infringements of this Regulation.

Finally, the Market Abuse Regulation allows Member States to provide for financial incentives to persons who offer relevant information about potential infringements of this Regulation to be granted in accordance with national law if those persons do not have other pre-existing legal or contractual duties to report such information. The conditions for the provision of incentives are that (1) the information is new, and (2) it results in the imposition of an administrative or criminal sanction, or the taking of another administrative measure, for an infringement of this Regulation.

---

A similar requirement to establish internal and external whistle-blowing mechanisms is also provided for in other EU legislation, such as in relation to MiFID II,\textsuperscript{11} undertakings for collective investment in transferable securities (UCITS),\textsuperscript{12} insurance distribution,\textsuperscript{13} and packaged retail and insurance-based investment products (PRIIPs).\textsuperscript{14}

Finally, this requirement also exists in relation to the activities and supervision of credit institutions. The details of this requirement are laid down in Article 71 of the 2013 EU Banking Directive.\textsuperscript{15} The whistle-blowing mechanism to be established thereunder is to encourage the reporting of potential or actual breaches of both the national provisions implementing the 2013 EU Banking Directive and the 2013 EU Banking Regulation.\textsuperscript{16}

As regards credit institutions in the eurozone, the European Central Bank (ECB) obviously has an essential supervisory role to play, being at the helm of the Single Supervisory Mechanism (SSM). As ‘competent authority’ in the meaning of the aforementioned Article 71, the ECB has set up a breach-reporting mechanism. The rules and procedures governing this mechanism are laid down in Articles 36 to 38 of the SSM Framework Regulation.\textsuperscript{17} They set forth that any person may, in good faith, submit a report directly to the ECB if that person has reasonable grounds for believing that the report will show breaches of the relevant EU law by the institutions supervised by the ECB or by the supervisors themselves (both the ECB and the national competent authorities for banking supervision, such as the National Bank of Belgium (NBB), i.e., the Belgian central bank and banking supervisor).\textsuperscript{18} All personal data concerning both the person who reports a breach and the person who is allegedly responsible for a breach shall be protected in compliance with the EU data protection framework.

\begin{enumerate}
\item The term ‘relevant EU law’ covers the substantive rules relating to the prudential supervision of credit institutions that the ECB applies when carrying out the tasks conferred on it by the SSM Regulation. These rules are composed of directly applicable EU Regulations such as the Capital Requirements Regulation. When EU Directives are considered relevant Union law, the national implementations of these Directives are also considered to be relevant Union law, e.g., national implementations of the Capital Requirements
\end{enumerate}
Also, the ECB shall not reveal the identity of a person who has made a report without first obtaining that person's explicit consent, unless disclosure is required by a court order in the context of further investigations or subsequent judicial proceedings.

With regard to significant supervised entities, that is, those entities that are directly supervised by the ECB, the ECB itself assesses the report. By contrast, with regard to less significant supervised entities, the ECB only assesses a report for breaches of ECB regulations or decisions. The ECB forwards reports concerning less significant supervised entities to the relevant national competent authority (e.g., the NBB in Belgium), without communicating the identity of the person who made the report, unless that person provides his or her explicit consent.

While everybody who has knowledge of a potential breach may report it to the ECB, the ECB has indicated that compliance officers, auditors and other employees of a bank are the groups that are most likely to have knowledge of possible wrongdoing. In 2018 the ECB received 124 breach reports, an increase of almost 40 per cent compared to the previous year.19 The breaches that are most commonly reported to the ECB concern the inadequate calculation of own funds and capital requirements, and governance issues within credit institutions.

National law on whistle-blowing in EU Member States: the example of Belgium

Belgian law does not contain general rules on whistle-blowing.20 However, particularly in relation to financial services and banking, Belgian law has implemented the relevant EU legislation.

Thus, Article 21, Section 1, No. 8 of the Belgian Banking Law contains a specific requirement that Belgian credit institutions must have an appropriate internal whistle-blowing system in place for the reporting of breaches of rules and codes of conducts.21 The external side of the whistle-blowing system is laid down in Article 36/7/1 of the Belgian Law of 22 February 1998 on the National Bank of Belgium.22 It governs, among others, the good faith reporting to the NBB of an actual or alleged infringement of the rules governing the status and supervision of credit institutions by an employee of the institution. We refer to what is mentioned above on the division of tasks within the SSM between the ECB and national supervisors, such as the NBB, and hence the circumstances in which Belgian law's whistle-blowing system comes into play.

The Law of 31 July 2017 has implemented in Belgian law the whistle-blowing mechanism that EU Member States are required to establish under EU legislation in areas such as market abuse, MiFID II, UCITS and PRIIPs. The rules governing the ‘external’ dimension of such mechanisms is now addressed in Article 69-bis of the Belgian Law of Directive IV. Furthermore, where directly applicable EU Regulations grant options to Member States, the national legislation exercising those options is considered to be relevant Union law. ECB regulations, such as the SSM Framework Regulation, and ECB decisions, are also considered to be relevant Union law.

20 Note, however, that on 29 November 2006, the Belgian Privacy Commission issued a non-binding recommendation setting out how a whistle-blowing system could be established in compliance with the Belgian Data Protection Law. Also, specific whistle-blowing rules apply to certain categories of civil servants.
21 In full: Law of 25 April 2014 on the status and supervision of credit institutions (Belgian Official State Gazette, 7 May 2014, p. 36794).
2 August 2002 on the supervision of the financial sector and the financial services – with the Belgian Financial Services and Markets Authority (FSMA) functioning as the authority to whom the reporting will need to be done\(^\text{23}\) – while the ‘internal dimension’ is laid out in Article 69-ter of this law.

Importantly, these provisions are not limited to implementing into Belgian law the requirements of the EU legislation but go beyond the areas covered by this legislation. Thus, they will introduce both the external and internal dimensions of the whistle-blowing mechanism in a ‘transversal’ manner (i.e., for the reporting of infringements of any of the rules for which the FSMA has supervisory powers). These rules are enumerated in Article 45 of the Law of 2 August 2002. They concern a wide variety of financial and related services and the institutions providing them. These whistle-blowing provisions address topics such as the duty of secrecy of the FSMA as regards the identity of the reporting person, the protection of this person against claims and sanctions, the protection of this person and of the person affected by the reporting (i.e., the author of the possible infringement) against retaliatory, discriminatory and other forms of unjust treatment, and the financial and other remedies that these persons benefit from in case of such treatment by their employer. Of course, this protection does not affect the possibility of, for example, the employer taking the appropriate measures and actions that are open under statutory law or the contract with regard to a person who has effectively committed an infringement, including when this infringement came to light as a result of reporting by the whistle-blower.

As indicated above, in competition law, the introduction of administrative fines for individuals goes hand in hand with the right for individuals to seek immunity on their own account, besides or alongside a leniency application from the company.

The coordination between these sectoral whistle-blowing rules and the future general rules that will implement the Whistle-blowing Directive into Belgian law remains to be seen.

III  ENFORCEMENT

i  Corporate liability and penalties

*Competition law*

Under EU competition law, the European Commission may impose fines on corporates of up to 10 per cent of the annual consolidated worldwide turnover of the undertaking. In setting the fine, the European Commission takes into account the gravity and duration of the infringement. The Fining Guidelines provide more guidance on how exactly the European Commission will calculate the fines.\(^\text{24}\) These Guidelines are not binding on the European courts, who exercise full jurisdiction and can review the fine. However, the instances where the European courts have adjusted fines in competition cases remain exceptional.

A similar system of sanctions is in place under Belgian competition law, albeit with some differences. Until recently, the maximum amount of the fine was set at 10 per cent of the consolidated turnover realised by the undertaking on the Belgian market and through exports from Belgium (and thus not the worldwide turnover). Since the Act of 2 May 2019,

\(^{23}\) The FSMA has adopted a regulation specifying the procedural rules applicable to receiving and processing of infringement alerts. This regulation was approved by the Royal Decree of 24 September 2017 (Belgian Official State Gazette, 28 September 2017, p. 89027).

\(^{24}\) Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No. 1/2003 (OJ C 210, 1 September 2006, p. 2).
fines may not exceed 10 per cent of the undertaking’s total worldwide turnover during the financial year preceding the sanction decision. However, the previous system continues to prevail for infringements committed before the Act of 2 May 2019 entered into force.\textsuperscript{25} The BCA may also impose interim measures and periodic penalty payments of up to 5 per cent of the average daily turnover for each day’s failure to comply with the decision. The BCA issued guidelines on the calculation of fines on 26 August 2014.\textsuperscript{26} These guidelines refer to the calculation method of the European fining guidelines described above. While the Belgian fining guidelines have no binding value, the courts have established that the BCA could not depart from the methods for the calculation of fines set out therein without violating the principle of legitimate expectations.

A 10 per cent reduction of the fine can be granted both under EU and Belgian competition law if an undertaking agrees to enter into a settlement with the competition authority. In doing so, the undertaking concerned must admit its involvement in the infringement.

In cases of private law claims, the regular courts may order the payment of compensatory damages for the harm that the competition law infringement caused to the claimants. Class actions have been introduced into Belgian law by legislation dated 28 March 2014, which entered into force on 1 September 2014. Adequate representatives are able to lodge collective claims on behalf of consumers for breach of contractual commitments or certain legal provisions, such as Book IV of the Belgian Code of Economic Law and some financial law regulations. Despite these procedural adjustments and the adoption of the Antitrust Damages Directive, it remains difficult for claimants to quantify the harm caused by a competition law infringement.

There are no criminal sanctions under Belgian law for competition law infringements.\textsuperscript{27}

**EU financial services and banking**

The SSM started in November 2014 and is one of the four pillars of the EU Banking Union. It is particularly relevant for the supervision of credit institutions in the eurozone. It is composed of the ECB and the national authorities that are competent for the supervision of credit institutions in their respective Member State (for instance, the NBB in Belgium). The ECB has a key role, as it is responsible for the effective and consistent functioning of the SSM. In addition, it has, among the thousands of credit institutions that are established in the eurozone, full and direct supervisory authority over ‘significant institutions’.

To ensure compliance with the supervisory rules and its regulations and decisions in this area, the ECB has significant supervisory,\textsuperscript{28} investigative and sanctioning powers.

The ECB’s investigative powers are similar to those that have been granted to other EU financial supervisory authorities, such as the European Securities and Markets Authority in the areas of the supervision of over-the-counter derivatives, central counterparties and trade

\textsuperscript{25} Belgian Official State Gazette, 24 May 2019, p. 50073.
\textsuperscript{26} Belgian Official State Gazette, 10 September 2014, p. 71456.
\textsuperscript{27} Some exceptions apply, e.g., bid rigging in public procurement and breaking of seals applied by the BCA.
\textsuperscript{28} e.g., requiring a credit institution to hold own funds in excess of the EU law capital requirements or to use its net profits to strengthen its own funds, requesting the divestment of activities that pose excessive risks to the soundness of an institution, limiting variable remuneration when it is inconsistent with the maintenance of a sound capital base, or removing members from the management of a credit institution.
Belgium

repositories,\textsuperscript{29} and of credit rating agencies.\textsuperscript{30} Thus, the ECB has the right to require legal and natural persons to provide all information that is necessary to carry out its supervisory tasks. It also has the right to require the submission and examination of documents, books and records, to obtain written or oral explanations from the representatives or staff of such persons, and to conduct all necessary on-site inspections at the business premises of the institutions under its supervision, including without prior announcement.

If an institution supervised by the ECB, intentionally or negligently, breaches a requirement under directly applicable EU law for which administrative sanctions are made available, then the ECB has the right to start a sanctioning procedure and impose administrative pecuniary sanctions.\textsuperscript{31} The same right exists in the case of breaches of regulations or decisions adopted by the ECB in the exercise of its supervisory tasks.\textsuperscript{32} The ECB also has the right to publish the imposition of such sanctions, irrespective of whether the decision has been appealed. However, in certain exceptional circumstances, publication may be anonymised or delayed.

In other cases – for instance, breaches of national legislation that transposes EU Directives – the ECB only has the option of requiring the national supervisory authorities to open a sanctioning procedure with a view to taking action to ensure that appropriate sanctions are imposed by the national authorities.

The ECB imposes its sanctions in accordance with the ECB Sanctioning Regulation,\textsuperscript{33} which, among others, sets forth the procedural rules and time limits for the imposition of sanctions, as well as their judicial review.

At the national level, the NBB in Belgium has the option to take a wide range of administrative measures. It has, through its Sanctions Commission, the power to impose administrative fines and penalties of up to €2.5 million per infringement, in cases of


\textsuperscript{31} The sanctions that the ECB can impose in this case consist of a maximum of twice the amount of the profits gained or losses avoided because of the breach where those can be determined, or a maximum of 10 per cent of the total annual turnover of that institution in the preceding business year. If the institution is a subsidiary, then the relevant total annual turnover is calculated on a consolidated basis.

\textsuperscript{32} The sanctions that the ECB can impose in this case consist of (1) fines of a maximum of twice the amount of the profits gained or losses avoided because of the infringement where these can be determined, or 10 per cent of the total annual turnover of the undertaking, and (2) periodic penalty payments of a maximum of 5 per cent of the average daily turnover per day of infringement. Periodic penalty payments may be imposed in respect of a maximum period of six months from the date stipulated in the decision imposing the periodic penalty payment.

non-compliance with the rules under its supervision. The specific procedural rules for
the imposition of these sanctions are laid down in Articles 36/9 to 36/11 of the Law of
22 February 1998 on the National Bank of Belgium. 34

The FSMA (the Belgian securities and markets supervisor) is also empowered to use
a wide range of administrative measures and, through the FSMA Sanctions Commission,
to impose administrative fines of up to €2.5 million per infringement, in the case of
non-compliance with the rules that fall under its supervision. The specific procedural rules
for imposition by the FSMA of administrative fines are laid down in Articles 70 to 72 of the
Financial Supervision Act, 35 as well as in the provisions of an internal regulation from the
Sanctions Commission of the FSMA of 18 September 2017. 36

Criminal proceedings

Within the European Union, criminal law is an area that still falls within the remit of the
respective Member States. Hence, the rules on whether a corporate can be criminally liable
and on the criminal sanctions in the case of such liability vary according to the Member State
concerned, including in areas that concern the transposition of EU Directives (for instance
on financial services and banking) that require Member States to establish such sanctions.

For instance, corporates in Belgium are, subject to certain conditions, criminally liable
for offences that are either intrinsically related to the accomplishment of their corporate
purpose or corporate interests or have been committed on their behalf. The criminal sanctions
that can be imposed on corporates may, among others, consist of fines, a confiscation of
corporate assets, winding up, a prohibition to exercise an activity, dismantling of company
branches and publication of the criminal judgment. As a corporate cannot be sentenced to
imprisonment, the penalty of imprisonment is converted into a fine in accordance with a
complex calculation mechanism.

ii  Compliance programmes

A compliance programme is considered neither a mitigating nor an aggravating circumstance
by the competition fining guidelines. It is, nonetheless, highly recommended for undertakings
to implement competition law compliance programmes, because they aim to reduce the risk
of contravention, facilitating immediate cessation of any potential infringing conduct (thus
minimising potential penalties), and earlier detection of any potential infringement (thus
providing the opportunity to apply for leniency where appropriate).

In the area of financial services, various statutory rules and guidelines by the regulators
require financial institutions to have appropriate compliance programmes. The absence
of a programme constitutes a regulatory breach, while the existence and effective use of
a programme – particularly in terms of compliance, training and monitoring – might, in
certain circumstances, constitute a defence or, at least, a penalty-mitigating factor.

The mere existence of a compliance programme does not automatically constitute
a mitigating circumstance under Belgian criminal law. However, its existence might be helpful
in, for example, the defence of senior managers that they do not have a personal criminal

liability, as they tried ensuring compliant behaviour through setting up internal compliance programmes, monitoring the effective functioning of these programmes and following up any issues reported through such programmes.

IV INTERNATIONAL

i Extraterritorial jurisdiction
Belgian competition law applies to any conduct that restricts competition on the Belgian market or a substantial part thereof. The place where the agreement or practice is implemented (irrespective of the registered office of the companies concerned) is relevant in this respect. Certain arrangements within the European Competition Network govern the allocation of cases between the national competition authorities of the EU Member States and the European Commission.

In July 2007, the Belgian financial markets supervisor rendered a landmark decision for the EU financial services landscape. This decision concerns the protection against double jeopardy, that is, the right of a person not to be prosecuted or punished more than once for the same acts (also known as the ne bis in idem principle). The Belgian regulator relied on Article 54 of the 1990 Schengen Agreement to refrain from imposing a sanction for behaviour that would otherwise have fallen within its jurisdiction. The practice under investigation related to possible market abuse by a financial institution based in the United Kingdom. The importance of Article 54 of the 1990 Schengen Agreement is twofold: the ne bis in idem principle is applicable to a cross-border context and it only requires the same facts (i.e., idem factum), and possible differences in the legal qualification of the breach are not relevant (hence, no requirement of idem crimen).

As a general rule, Belgian criminal courts have jurisdiction if the offence is committed in Belgium. A crime or offence is considered to have been committed in Belgium if one of its constitutive elements took place on Belgian territory. However, an offence committed on foreign state territory might be punishable before the Belgian courts in certain circumstances (e.g., bribery).

ii International cooperation
The Belgian Competition Authority does not have investigative powers outside Belgium. Thus, investigations concerning companies located outside Belgium will require cooperation with the competition authorities of other jurisdictions. Within the European Competition Network, cooperation between the European Commission and the national competition authorities of EU Member States is based on the provisions of EU Regulation No. 1/2003.37 The Belgian Competition Authority has the power to exchange all information (even if confidential) with the European Commission and the national competition authorities of other EU Member States, who may also ask the Belgian competition prosecutors for assistance in inspections that are carried out pursuant to EU Regulation No. 1/2003. On 22 March 2017, the European Commission presented a proposal intended to empower Member States’ competition authorities to be more effective enforcers and to ensure the

---

proper functioning of the internal market. The proposal recognised the key role of the national competition authorities (NCAs) in the enforcement of European competition law rules, the NCAs being responsible for 85 per cent of the more than 1,000 enforcement decisions. Hence, it aimed to ensure that when applying the EU antitrust rules, NCAs had the appropriate enforcement tools, with minimum guarantees and standards, to bring about a genuine common competition enforcement area. The proposed Directive was adopted on 11 December 2018.

Likewise, financial services and banking supervisors and regulators are often, by virtue of EU or national legislation, in many areas able to exchange information with their foreign counterparts, without the exchange giving rise to a breach of the regulators’ confidentiality obligation. Similarly, in various areas, these supervisors and regulators have the statutory authority to cooperate with their foreign counterparts. Particularly within the European Union, this cooperation may include on-site inspections by a foreign regulator in Belgium or vice versa, including for practices that may constitute a breach of foreign law but not the law of the place where the inspection is carried out. In 2018, the FSMA received 17 requests for international cooperation from competent foreign supervisory authorities. The requests often relate to the identification of the beneficiary of an operation. The same year, the FSMA sent 44 requests for cooperation to foreign competent authorities, compared to 30 in 2017.

As Belgium is a member of the European Union, it is bound by EU legislation, as well as the 1990 Schengen Agreement and various other international agreements on extradition and cooperation in criminal matters. In addition, Belgium has concluded several bilateral and multilateral treaties in this respect, including the Benelux Extradition Treaty of 27 June 1962. Belgium has also enacted the Act of 9 December 2004 on mutual international legal assistance in criminal proceedings, according to which it will offer its assistance to foreign investigations on Belgian territory. These investigations will be conducted in accordance with Belgian law and under the authority of the public prosecutor or examining magistrate.

V YEAR IN REVIEW

In 2017, there was an increased activism of the regulators, particularly financial regulators such as the ECB and the FSMA. As regards the latter, we see a focus on regulatory action in Belgium that is intended to, or at least results in, a settlement between the supervised entity and the FSMA. While such a settlement brings an end to the investigation, it is typically published in a non-anonymous manner with increasingly high settlement amounts that the entity needs to pay and with commitments from that entity on how it will deal with customers that were potentially affected by the behaviour that is the subject matter of the settlement. It is expected that this trend will continue going forward. In 2019, the FSMA proposed 13 settlements for a total amount of €2,399,143.56.

38 Proposal for a Directive of the European Parliament and of the Council to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market (COM/2017/0142 final – 2017/063 (COD)).

39 Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market (OJ L 11, 14 January 2019, p. 3).
INTRODUCTION

Brazilian criminal procedure law establishes that the investigation of the origins and content of crimes committed within or by companies may be carried out by federal and state civil police forces. It is also possible that the Public Prosecutor’s Office (at state or federal levels) will carry out its own investigation. Nevertheless, in both situations, judgment of the case rests with the courts. Police officers, public prosecutors and members of the court have discretionary powers to conduct cases free from external influences, so long as the conduct of these authorities respects the guarantees of due process and the right to privacy.

In the context of administrative offences, companies and their employees and executives can also be investigated by other bodies, such as parliamentary investigation committees (at local, state and federal levels), which have subpoena powers, and by audit tribunals (again at local, state and federal levels), which are empowered to investigate wrongdoing in public administration.

Concerning incidents of corruption within public administration, Decree No. 8,420/15, which regulates the Brazilian Anticorruption Law (Law No. 12,846/13), provides that the investigation of civil and administrative liability rests with the highest authority of the aggrieved entity. To assess where responsibility lies, the entity must start a preliminary investigation and, based on the evidence gathered, the competent authority may determine the commencement of the administrative procedure by which any sanctions on the entity under investigation may be established. A finding of guilt is always subject to judicial review.

Even though private agencies and investigators are authorised to operate in Brazil, they do not have special powers of investigation (e.g., to force people to give testimony or produce evidence), but they can collect evidence to the extent that it does not violate any rights of the targeted individuals, such as privacy, freedom of movement and property.

Law No. 13,432/17 provides the legal basis for those working as private investigators, especially in relation to how those professionals may influence the gathering of evidence by public authorities. In this sense, there can be cooperation, by which evidence uncovered through private efforts can be submitted to the authorities, as long as the evidence has been obtained within the tenets of the law. Pursuant to this law, companies and individuals are

---

1 João Daniel Rassi is a partner, while Victor Labate and Pedro Luís de Almeida Camargo are associates at Siqueira Castro Advogados.
2 Mostly, the competence of federal justice is provided under Article 190 of the Brazilian Federal Constitution.
3 Federal Supreme Court (STF), RE 593.727.
4 Article 4 of Decree No. 8,420/15.
5 Article 5 of Law No. 13,432/17.
legally allowed to cooperate with the authorities by providing evidence gathered as part of an internal investigation. However, this Law establishes in its Article 5, sole paragraph, that the public authority in charge of the investigation may accept or reject the private investigator’s assistance.

Even though this is not explicitly provided in Law, attorneys can also conduct private investigations, according to the Brazilian Bar Association in its Resolution No. 188/2018. The Bar Association states that the possibility of conducting private investigations does not require legislative authorisation, as it is already included in the general powers of client representation. Nevertheless, this stance has faced some criticism from public authorities, such as police chiefs and investigators.

Although the Brazilian judicial system is designed to avoid situations where the public may have influence over decisions (for example, judges are not elected and jury trials are restricted to wilful murder cases), experience shows that political agendas may interfere with prosecutions, especially regarding cases of corruption in which public opinion is intensified owing to, for example, Operation Car Wash developments.

II CONDUCT

i Self-reporting

As a rule, private companies are not required to report offences committed by their employees to the authorities. However, the Money Laundering Law (Law No. 9,613/98) lists the individuals and legal entities engaged in business activity that are required to communicate to the Council for Control of Financial Activity, within 24 hours, all transactions suspected of involving money laundering (Article 11.II.b). In general, the parties so obliged are individuals and legal entities that – permanently or occasionally, primarily or secondarily – engage in activities connected with the following markets: finance, real estate, luxury goods, sports or arts, transport of valuables and livestock breeding.

Under the Money Laundering Law, no benefit is obtained by those who comply with their reporting duties. However, the public authority may impose more severe penalties on those who fail in the duties required under Article 12 thereof. For those accused of money laundering, it is possible to obtain leniency by voluntarily collaborating with the authorities, providing information about the crime, identifying the other perpetrators, and so on. As a consequence of collaborating with the authorities, a shorter jail term or a sentence of probation may be imposed (or less severe conditions, such as a minimum security prison or authorisation to work during the daytime).

6 The situation is different in the public sector, where the duty to report suspected criminal behaviour applies to federal civil servants, as per Law No. 8,112/90.
7 The law covers crimes of money laundering, concealment of assets and use of the financial system for commission of crimes, and created the Council for Control of Financial Activities, among other things.
8 It is possible for the parties who fail to inform the suspect transactions to face charges for complicity in money laundering, although the theme of criminal liability of compliance officers for omission is still polemical in Brazil.
9 The list, which is comprehensive, can be found in Article 9 of Law No. 9,613/98.
10 Among the penalties established in the law are warning, fine, temporary ineligibility to hold management positions and cancellation or suspension of authorisation to engage in activity, operation or functioning.
11 Article 1, Section 5 of Law No. 9,613/98.
Other laws also allow for leniency, called ‘collaboration agreements’.\textsuperscript{12} In fact, any individual accused of engaging in organised crime in Brazil can collaborate with the authorities in return for a lighter sentence or other benefits (Articles 4 to 7 of Law No. 12,850/13).

In the area of antitrust law, taking part in a cartel is both an administrative\textsuperscript{13} and criminal\textsuperscript{14} offence. Although there is no obligation to report such behaviour by individuals or companies, both can be eligible for benefits by cooperating, in the criminal sphere (individuals only) or the administrative sphere. According to Article 86 of Law No. 12,529/11, companies and individuals that enter into leniency agreements can have their administrative penalties reduced by a third to two-thirds in return for cooperating in identifying and producing evidence against the other participants of the cartel.\textsuperscript{15}

With respect to the criminal liability, Article 87 of the same law establishes that a leniency agreement also prevents criminal charges from being brought against individual signatories, but suspends the running of the time bar of crimes against the economic system (Article 4 of Law No. 12,529/11) and related crimes,\textsuperscript{16} such as fraud in bidding processes and criminal conspiracy.\textsuperscript{17} Because companies are not criminally liable for cartel offences, there is no criminal benefit involved for the corporation in leniency agreements.

The recently passed Law No. 13,506/17 also provides for the possibility of companies and individuals signing leniency agreements with the Central Bank of Brazil and the Securities and Exchanges Commission with regard to financial offences or conduct that jeopardises investors’ and shareholders’ interests, respectively.

The granting of these benefits by the authorities responsible for establishing the collaboration agreement and the leniency programme is subject to the authorities’ subjective evaluation. The lack of objective parameters is often criticised by legal entities.

\textbf{ii Internal investigations}

Companies that receive denunciations or suspect irregular behaviour by their employees can conduct their own investigations to identify the facts and impose penalties on those found responsible.\textsuperscript{18} They can also engage external advisers, private detectives or audit firms

\textsuperscript{12} Rewarded denunciation is also applicable to the crimes committed against the national financial system (Law No. 7,492/86, Article 25, Section 2), tax crimes (Law No. 8,137/90, Article 16), drug trafficking (Law No. 11,343/06, Article 41) and kidnapping (Penal Code, Article 159, Section 4).

\textsuperscript{13} Law No. 12,529/11. Administrative and criminal spheres are autonomous even though, in some cases, the collaboration in the administrative sphere can reflect in the criminal area (e.g., the leniency agreement). In this sense, considering that benefits from the law can reflect in the two different areas and their interest towards investigation is mutual, the Administrative Council for Economic Defence and the Federal Prosecutor’s Office of Cartel Combat signed the Memorandum No. 1/2016 to strengthen their cooperation.

\textsuperscript{14} Article 4 of Law No. 8,137/90.

\textsuperscript{15} ‘Cease and desist agreements’ are also available for companies willing to cooperate with the Competition Authority that did not come first to the organ.

\textsuperscript{16} In its last Peer Review on Competition Law and Policy in Brazil, the Organisation for Economic Co-operation and Development recommended modification of the leniency programme to eliminate the exposure of leniency participants to prosecution under criminal laws other than the Economic Crimes Law. Concerning non-related crimes, it is possible for the defence, upon confession, to request a reduced criminal penalty under Article 65(III)(d) of the Brazilian Penal Code.

to conduct investigations. As a rule, the investigation should involve as few people as possible to protect those implicated and to preserve the investigation itself. For this purpose, all those involved are typically asked to sign a confidentiality undertaking.\textsuperscript{19}

Audit reports, spreadsheets, official emails\textsuperscript{20} and transcripts of interviews are examples of evidence that can be gathered during this kind of investigation. During the proceedings, the suspect is entitled to retain a lawyer to be present at interviews, and while there is no legal requirement, the lawyer is permitted to see internal documents regarding the investigation that are related to the client.

Generally, this kind of investigation is conducted by external counsel, or by internal counsel assisted by external professionals, to ensure the impartiality of proceedings. At the end of the investigation, a report should be prepared outlining the case and the findings regarding the alleged irregularities and the wrongdoers involved, as well as proposing solutions and recommendations depending on which law has been infringed, and any possible penalties to be applied.\textsuperscript{21} Although it is not mandatory to submit the content of the report to the public authorities, courts may require it to be presented and, unless publication of the information presents a risk to the company, that order may be fulfilled.

Finally, attorney–client privilege still applies to investigations conducted by companies, owing to the broad scope established by the Brazilian Bar Association Statute. However, because this is a disposable right, the right to secrecy can be waived by the client; for instance, if the accused person wishes to benefit from collaboration with the company. In situations like this, it is recommended that the individual and the company are represented by a counsel to avoid any allegations of coercion or abuse of rights by both sides.

\textbf{iii Whistle-blowers}

A whistle-blower, by definition, is an individual who denounces a fact that is perceived to be illegal or improper within the company or public agency for which he or she works, without being involved in the allegedly criminal conduct.\textsuperscript{22}

The enactment of the Anti-Crime Bill through the Law No. 13,964/19 has enabled better regulation of the whistle-blower mechanisms that were introduced by Law No. 13,608/18, which solely authorised states to establish denunciation channels through which citizens could provide information regarding crimes or administrative offences against the public interests. If the information proves to be useful for the prevention or repression of offences, rewards may be granted.

Due to the alterations made by the Law No. 13,964/19, whistle-blowers are granted the right to anonymity, which can only be overridden when there are ‘relevant public interests’ or ‘concrete interests for the investigation’ involved (Article 4-B).

\begin{footnotes}
\footnotetext[19]{ibid.}
\footnotetext[20]{The best policy is to both specify the rule in the code of conduct and require all employees to sign a consent form when hired.}
\footnotetext[21]{Depending on the gravity of the act, the employee can be dismissed with or without cause, under the situations described in Article 482 of the Consolidated Labour Law (Decree-Law No. 5,452/43).}
\footnotetext[22]{Whistle-blowers should be differentiated from those who in some way have participated in or contributed to the crime and decide to cooperate with the authorities in return for leniency, as in the case of rewarded collaboration (V Greco F, Comentários à Lei de Organização Criminosa, São Paulo: Saraiva, 2014).}
\end{footnotes}
Besides ordinary witness protection rights, which are brought under Law No. 9,807/99, whistle-blowers are also granted the protection against retaliation (e.g., unjustifiable post replacement, financial sanctions and arbitrary dismissal) (Article 4-C).

III ENFORCEMENT

i Corporate liability

Companies can be held civilly liable for the acts of their employees in three situations, two general and one specific: by reason of culpa in eligendo (poor choice of those entrusted with performance of obligations); by reason of culpa in vigilando (insufficient oversight of the performance of obligations); and when an employee commits an act injurious to public administration, in Brazil or abroad.

The first and second situations of corporate responsibility are provided under Article 932, III of the Brazilian Civil Code and Súmula\(^{23}\) 341 from the Federal Supreme Court.\(^{24}\) The third situation, above, is a new form of corporate responsibility established by the Anticorruption Law (Law No. 12,846/13), which contains provisions on strict civil and administrative liability for acts that are harmful to national or foreign public administration.\(^{25}\)

Civil and administrative corporate liability under this provision does not preclude the personal liability of the individuals involved in such conduct.\(^{26}\)

Criminally, companies can only be held liable for environmental crimes, regardless of the individual responsibility of their agents. Article 3 of the Environmental Crimes Law (Law No. 9,605/98) establishes that companies shall be held criminally liable in cases of environmental offences committed ‘by decision of their legal or contractual representative, or collegiate body, in the interest or benefit of the entity’.

Finally, there is no legal impediment for the company and employees to be represented by the same lawyer, in either administrative or criminal proceedings. This will depend on the situation; namely, if there is no possible conflict of interest.

ii Penalties

The possible penalties will depend first of all on the category of culpability, among those defined above. For situations of culpa in vigilando or culpa in eligendo, the company will be liable for damages in proportion to the loss caused.

In relation to practices injurious to a national or foreign governmental entity, according to Article 19 of the Anticorruption Law, a company can be liable to the following penalties:

\(a\) seizure or forfeiture of money, rights or other assets gained directly or indirectly from the infraction, with reservation made for the rights of injured parties or third parties who acted in good faith;

\(b\) partial suspension or interdiction of activities;

\(c\) prohibition from receiving incentives, subsidies, donations or loans from governmental entities or official financial institutions, for between one and five years; or

\(^{23}\) A súmula is a statement of consolidated position, or jurisprudence, from a higher court.

\(^{24}\) The culpability of the employer or principal for the acts of the employee or agent is presumed.

\(^{25}\) The list of injurious acts is contained in Article 5 of Law No. 12,846/13.

\(^{26}\) Article 3, Section 1 of Law No. 12,846/13.
compulsory dissolution, when the company is found to have habitually facilitated or engaged in illegal acts or was incorporated to conceal illicit interests or the identity of the beneficial owners.

According to Articles 21 to 24 of the Environmental Crimes Law, the penalties applicable to companies for the practice of environmental crimes are:

- fines;
- partial or total suspension of activity;
- temporary interdiction of an establishment, project or activity;
- prohibition from contracting with governmental entities or obtaining subsidies or donations from them;
- payment for environmental programmes of projects;
- reclamation of degraded areas;
- maintenance of public spaces;
- contributions to public environmental or cultural entities; or
- forced liquidation, with the assets realised being transferred to the National Penitentiary Fund.

### Compliance programmes

The Environmental Crimes Law does not provide for any leniency regarding penalties for companies that have compliance or integrity programmes. Rather, it establishes that the penalty must be set in light of the gravity of the infraction, its motives and the consequences for public health and the environment, as well as the antecedents regarding compliance with environmental laws or regulations, and the economic situation of the company.27

The situation is different regarding civil and administrative liability for harmful acts against national or foreign governmental entities. The Anticorruption Law specifies that in applying penalties, the parameters of the sanction must be established by considering the existence of functional internal mechanisms and procedures for integrity, auditing, any incentive for the denunciation of irregularities, and the effective application of codes of ethics and conduct within the company.28

The parameters for evaluating a compliance programme are listed under Article 42 of Decree No. 8,420/15. These provisions include the existence of periodic training for employees concerning the scope of the company’s integrity programmes, the existence of independent structures for application of the integrity programme, the use of disciplinary measures in the event of violation of the programme’s provisions, and the transparency of any donations made by the companies to political parties, among others. These provisions are used as a guide for organisations when creating or reviewing compliance programmes.

Therefore, the existence of compliance programmes must be taken into consideration when imposing administrative or civil penalties for acts deemed injurious to public administration, by express provision of the Anticorruption Law. In the environmental sphere, there is no such provision, but this does not preclude consideration in this respect by the judge when imposing punishment.29

---

27 Article 6 of Law No. 9,605/98.
28 Article 7, VIII of Law No. 12,846/13.
29 In this respect, the Environmental Crimes Law allows reduction of penalties for ‘prior communication to the agent regarding the imminent risk of environmental degradation’, as well as for ‘collaboration with
iv Prosecution of individuals

Besides the prosecution of individuals for administrative, civil or criminal liability as discussed above, a company can dismiss a person from their job — even if dismissal is not mandatory for the matter in question — if the public authorities seek to hold the individual liable or in the case of an existing investigation against that person.

On the other hand, if there is no conflict of interest, the company can help its employee’s defence by presenting documents, depositions, etc. Indeed, it is common for companies to pay the legal costs of this defence, depending on whether there is a conflict of interest.

IV INTERNATIONAL

i Extraterritorial jurisdiction

Brazil’s Antitrust Law (Law No. 12,259/11) applies to the conduct of individuals and companies outside the country in cases when the practices took place integrally or partially inside the national territory, or the consequence of the practices produces or might produce effects in Brazil.31

Concerning the latter situation, the possibility of extraterritorial application of Brazilian law requires the potential injury caused by the conduct to be real and effective, not just hypothetical, or there will be no configuration of a crime.32

Likewise, the Anticorruption Law allows civil and administrative penalties to be applied to Brazilian individuals or companies that commit crimes against foreign governmental entities, even if the crime is committed abroad.33

In the criminal sphere, the rule in Brazil, as in many other countries, is of territoriality, by which Brazilian criminal laws apply only to acts committed in the country, with the only exceptions being:

a crimes committed against the life or freedom of the president;
b crimes committed against the property of public entities, the Brazilian state, the federated states and the municipalities;
c crimes committed against the public administration; and
d crimes of genocide when the criminal is Brazilian or resident in Brazil, and for crimes that Brazil is obliged to repress owing to international treaties and conventions.34

30 The jurisprudence from the labour courts takes the position that an employee can only be discharged for cause owing to commission of a crime after a final guilty verdict. However, the company can fire employees for cause based on other grounds, such as malpractice or administrative improbity, which are not crimes.
31 Article 2 of Law No. 12,259/11.
33 Article 28 of Law No. 12,846/13. See, in this respect, V Greco F, JD Rassi, O combate à corrupção e comentários à lei de responsabilidade de pessoas jurídicas (Law No. 12,846, of 10 August 2013), São Paulo: Saraiva, 2015, p. 214.
34 Article 7 of the Penal Code.
ii International cooperation

The Brazilian government can apply the law of other countries by means of passive international legal cooperation, which consists of the practice of national public acts that are instrumental in the functioning of foreign jurisdictions. This cooperation exists in three forms: direct (direct and immediate contact between the authorities of the two countries), indirect (through an intermediary for processing of requests) and direct assistance (postulation, through an intermediary, of a national decision for the benefit of the requesting state, in substitution of it).

Countries that cooperate with each other generally have treaties to that effect. However, the absence of a bilateral accord does not preclude cooperation by the Brazilian government with foreign governments. In these cases, the solicitation must be sent to the Superior Tribunal of Justice via a letter rogatory, and if the matter cannot be decided there, it will be sent to the Ministry of Justice for the necessary steps to be taken to provide direct assistance.

Extradition is common and is regulated by the Migration Law (Law No. 13.445/17). For extradition to be granted, it is necessary for certain conditions to be met, including that the act be considered a crime both in Brazil and in the requesting state, that the prospective person to be extradited is a foreigner and that there is a treaty or convention signed with Brazil or, if none exists, a promise of reciprocity by the foreign government.

The Federal Supreme Court has original jurisdiction over extradition requests, according to Article 102, I(g) of the Federal Constitution, which is why its final decision is not subject to appeal.

iii Local law considerations

As has already been stated, Brazil adopts the principle of territoriality as a rule for application of criminal law, both substantive and procedural, although there are exceptional situations in which local law can be applied to crimes committed by Brazilians abroad. Therefore, if the Brazilian justice system has jurisdiction to judge a certain crime even though it has been committed abroad, the procedural rules applied will be those of the Brazilian Criminal Procedure Code.

Brazilian higher courts have a consolidated approach concerning the existence of *lis alibi pendens* investigations in the sense that the closure of investigations being carried out by Brazilian public authorities may not occur under ordinary instances, provided that the

---

35 Such as the bilateral and multilateral accords on mutual assistance in criminal matters listed on the website of the Federal Prosecution Service: www.internacional.mpf.mp.br/normas-e-legislacao/tratados/tratados-de-mutual-legal-assistance-auxilio-juridico-mutuo-em-materia-penal.
37 On this theme, see the publication (in Portuguese) by the Federal Supreme Court at www.stf.jus.br/arquivo/cms/bibliotecaConsultaProdutoBibliotecaBibliografia/anexo/extradicao_nov2009.pdf.
admissibility test of a foreign sentence depends on analysis of the Superior Justice Tribunal. By determining the closure of the investigation on such basis, the ordinary judge would be anticipating the analysis of a higher court.

Likewise, if another state is competent to judge a crime committed by a Brazilian national, its own procedural rules will apply, even if they are in conflict with Brazilian guarantees. On this point, international treaties and conventions on human rights come to the fore, by establishing protection and a guarantee of the rights of individuals facing prosecution in another signatory state. Hence, for example, personal and banking data are protected by secrecy and may only be disclosed by court order, pursuant to the constitutional principle of privacy and private life (Article 5, X of the Constitution). If any such information is obtained illegally, it will not be admissible in court.

V YEAR IN REVIEW

The Anti-Crime Bill presented by the Minister of Justice and Public Safety, Sérgio Moro (former judge responsible for the Operation Car Wash cases), was passed by the Congress and turned into Law No. 13.964/19, providing a series of changes in criminal law and criminal procedure law, like the rising of the maximum period a person can stay arrested (from 30 to 40 years) and the requisites for downgrading incarceration conditions, as well as the aggravation of the applicable penalties for crimes involving violence. The law also created a new procedural mechanism allowing for plea bargains to be concluded between the Public Prosecution Office and the person to be charged, to avoid the pressing of criminal charges. The requisites for receiving the benefit are that the crime must have a maximum penalty of less than four years and must not involve the use of violence, nor can the person be a recidivist. After homologation by the judicial system, the person must fulfil the obligations set out in the agreement and, having concluded that he or she will be free from the criminal charges, reason why the facts won’t go to trial and there will be no convictions arising from it.

It is worth mentioning, on the other hand, that some alterations that were present in the original bill, such as the possibility of plea bargaining involving jail time, were removed by Congress. The legislators also included changes in the legislation that strengthened suspects’ rights and guarantees – such as establishing that the judge with jurisdiction over the investigation cannot be the same that will issue a verdict– which weren’t on the original bill.

Besides the legal changes taken over the course of 2019 and 2020, changes occurring within the Brazilian Financial Intelligence Unit (COAF in its Portuguese acronym) should be noted. It was firstly transferred from the Ministry of Economy to the Ministry of Justice and Public Safety and later returned to the Ministry of Economy linked to the Brazilian Central Bank. Its final transfer was justified because it would allow for a better synchrony between the regulatory agency for banks and the intelligence unit on the prevention of money laundering and terrorism financing.

Also, the Brazilian Supreme Court has restored its classic jurisprudence regarding the necessity of waiting the conviction sentence to become unappealable in order to commence

38 See, in this respect, the American Convention on Human Rights (Decree No. 678/92) and the International Covenant on Civil and Political Rights (Decree No. 592/92).

39 Some argue that a court order is not necessary to obtain basic listing information such as name, address and telephone number, only a command from a police authority.

40 Article 157 of the Criminal Procedure Code and Article 5, LVI of the Federal Constitution.
the sentence serving and thus making it illegal to determine the sentence serving whether the person was convicted by the Court of Appeals but there are pending appeals to the Superior Court of Justice or to the Brazilian Supreme Court. Another Supreme Court decision worth mentioning is the one regarding the level of secrecy in Financial Intelligence reports produced by COAF. After an initial decision suspending all proceedings in which there was tax or banking information exchanged directly between the Financial Intelligence Unit and public authorities (prosecutors and the police), the court ruled that there is no need for judicial authorisation in those cases and allowed the suspended proceedings to continue.

VI CONCLUSIONS AND OUTLOOK

The criminal scandals involving the family of the President Jair Bolsonaro, such as the possible illicit funding of the 2018 political campaigns, his family's close relation to members of criminal organisations and militias from Rio de Janeiro, accusations of interference in the Federal Police Department and the evidence of the practice of money laundering by one of his sons have taken over the news, overshadowing the activities that are still being carried out in the context of Operation Car Wash. The conflict over the president's interference over the federal police led to Minister Sérgio Moro’s resignation and unleashed an investigation over Jair Bolsonaro’s actions, which is currently ongoing.

The high costs of implementation and low efficiency of the traditional forms of investigation have been the basis for a still-growing demand for consensual mechanisms of conflict resolution by the public authorities (from administrative and judicial organs), like leniency agreements, collaboration agreements, plea bargains, etc. Most of these mechanisms still lack a more detailed regulation, to provide more security to the citizens with regard to what to expect from these organs as benefits and the standard of evidence required.

Due to the social impacts caused by the covid-19 pandemic, the government has decided to postpone the deadlines for the implementation of the integrity programmes established for the banks and institutions authorised by the Brazilian Central Bank in the context of money laundering and terrorism financing prevention (according to DC/BACEN No. 3.978) and regarding data protection (according to Federal Law No. 13.709/18).
I  INTRODUCTION

Government investigations in China can be generally divided into two major categories: criminal investigations and administrative investigations, with the investigative power being vested among multiple authorities. From a criminal perspective, authorities with criminal investigative power include:

- public security bureaus (PSBs), responsible for investigations, criminal detentions, the execution of arrests and preliminary inquiries in criminal cases;
- the people’s procuratorates (procuratorates), responsible for prosecutions, the approval of arrests and conducting investigations on criminal violations relating to a judicial functionary’s infringement on citizens’ rights or judicial justice;
- supervisory commissions, which supervise all public officials, investigate duty-related illegal activities and offences, and carry out anti-corruption work;
- national security authorities, which investigate and handle cases of crimes that compromise national security, performing the same functions and powers as PSBs;
- military security authorities, which may exercise the right to investigate criminal cases occurring in the military;
- the China Coast Guard, a law enforcement body that safeguards marine rights and exercises the right to investigate criminal cases occurring at sea; and
- prisons.

From an administrative perspective, authorities with investigative powers include:

- the State Administration for Market Regulation (SAMR), which oversees market regulation, food safety, healthcare compliance, advertisement violations, competition violations, commercial bribery, anti-monopoly, etc.; and its subsidiary bureaus, including the administrations for market regulations (AMRs) at the provincial, municipal and county levels;
- the National Development and Reform Commission and its subsidiary bureaus, responsible for overall planning and control of the national economy, and investigating price-related violations;
- the China Securities Regulatory Commission (CSRC) and its subsidiary bureaus, responsible for the administration of securities and investigating securities fraud;

1 Alan Zhou and Jacky Li are partners at Global Law Office.

2 PSBs are empowered with dual investigative authorities at both criminal and administrative levels.
PSBs, which are also responsible for investigating administrative violations impacting public security; and

e the People’s Bank of China (PBOC) and its subsidiaries, responsible for carrying out monetary policy and regulation of financial institutions in mainland China, and regulating money laundering activities;

f other administrative authorities, such as the State Taxation Administration, the Customs, and the Environmental Protection Bureaus, etc.

For criminal investigations, the authorities are empowered to:

a interrogate the criminal suspect;

b interview with the witnesses;

c inspect or examine the sites, objects and persons relevant to a crime (including dawn raids);

d search the criminal suspect and his or her belongings and residence, and anyone who might be hiding a criminal or criminal evidence, as well as other relevant places;

e seal up or seize the property and documents; and

f access or freeze a criminal suspect’s deposits, remittance, bonds, stocks, shares, funds or other property.

For administrative investigations, the authorities are generally empowered to:

a conduct on-site inspections (including dawn raids);

b interview the parties involved in the suspected violation;

c require the parties involved in the suspected violation to produce relevant supporting documents;

d review and reproduce documents and materials;

e seal up or seize property; and

f access bank accounts.

Government investigations may be triggered by routine inspections, whistle-blowing reports, accusations, complaints, self-disclosure, transfers of cases among authorities, or even media exposure related to certain misconducts. Once a government investigation has commenced, the responsible authorities will assert the discretion over the investigation methods depending on the nature of the alleged misconduct and the available resources for investigation.

Among the enumerated investigation methods, dawn raids are adopted quite frequently by government authorities. A dawn raid may be carried out if the authorities believe that prior notice or warning could possibly lead to the destruction or falsification of evidence. During a government dawn raid, the officers will show up without prior notice, usually in the morning at the start of the working day at the pre-determined sites. Several sites can be targeted simultaneously within or across provinces and a dawn raid can last for several days. Government authorities may have already collected evidence through peripheral investigations before initiating a dawn raid or sometimes a dawn raid could be triggered under exigent circumstances.

The time frames for government investigations are usually set in the respective laws and regulations, varying among the authorities. Companies under investigation are obliged to cooperate with the authorities and it is crucial to timely evaluate the potential legal implications and conduct necessary interactions with the authorities to contain the legal risk exposures and to achieve a favourable result.
II CONDUCT

i Self-reporting

Article 110 of the Criminal Procedure Law imposes a general obligation on individuals and entities to report any suspected crimes or criminal activity, but from a literal interpretation, the requirement is construed from the general public perspective to report criminal activities of others, instead of self-reporting, and no legal consequences are clearly stipulated for failing to self-report. Article 67 of the Criminal Law to some extent encourages self-reporting of criminal activity by stipulating mitigation or even exemption from the criminal penalties under voluntary confession circumstances. Similar principles could also be reflected in some other provisions prescribed in the Criminal Law. For example, Article 164 of the Criminal Law provides that ‘any briber who confesses the bribery voluntarily prior to prosecution may be given a mitigated punishment or be exempted from punishment’. Article 28 of the Counter-Espionage Law provides that:

whoever joins a hostile or espionage organisation abroad under duress or inducement to engage in activities compromising the national security of China, but that honestly states the fact to a mission of China abroad in a timely manner or, after his or her return from abroad, honestly states the fact directly, or through his or her employer to a national security authority or a public security authority in a timely manner and shows repentance, may be exempted from legal liability.

From the administrative law perspective, self-reporting obligations are scattered in various laws and regulations, mostly related to violations that might have impact on social security and public welfare, such as food and drug safety, environmental protection and cybersecurity. For example, Article 47 of the Food Safety Law requires food manufacturers or business operators to cease food manufacturing or food business operations, and report to the food safety supervision and administration departments in the event of a food safety incident with potential risks. For other administrative violations, self-reporting is now appearing more often as a prerequisite in certain leniency programmes for companies to receive self-disclosure or cooperation credit. A typical situation is a horizontal monopoly agreement case, where business operators could choose to self-disclose the violation and provide important evidence in exchange for lenient treatment.

ii Internal investigations

Conducting internal investigation in general is not a statutory obligation in China except otherwise prescribed in the legislation applicable for specific industry, mostly in response to safety incidents. For instance, the Administrative Measures for Medical Device-Related Adverse Event Monitoring and Re-evaluation provides that, after identifying a medical device-related adverse event, marketing authorisation holders must immediately cease sales and operations, notify the user, in parallel with conducting an investigation and self-inspection on manufacturing quality control systems, and report the findings to the supervision authorities.

In addition, Chinese authorities (often industry supervision authorities) may initiate enforcement actions and require companies to conduct self-inspections and report non-compliant activities. For instance, in an ad hoc enforcement against commercial bribery
in the healthcare industry, initiated by the AMRs in Tianjin in 2017 and 2018, companies and medical institutions were required to conduct self-inspections on commercial bribery and take corresponding remedial actions in this regard.

In practice, internal investigations are incorporated into the internal control mechanism by companies for compliance purposes. The cause of the actions varies in each company but white-collar crime and fraud (e.g., commercial bribery, bid rigging and embezzlement) are usually among the focuses for the majority of companies in China.

Commonly, internal investigations are undertaken by in-house counsels in the company or external local counsels depending on the nature and severity of the issues under investigation. The methodology and process for these internal investigations usually include document review, financial review and interviews with employees and other personnel. The key issues during internal investigations involve the legal issue identification, design and implementation of the investigation process analysis based on the findings and determining the solutions. Notably, due process and evidence preservation are often overlooked by companies, as it is very likely that the facts and evidence gathered under internal investigation may end up in labour arbitration tribunals or court for litigation purposes or be submitted to the Chinese authorities. Therefore, how to preserve the integrity of the internal investigation and ensure the admissibility of the evidence should be carefully evaluated during the preparation and implementation of the internal investigation.

Companies in China also commonly conduct internal investigations for foreign law considerations, such as the Foreign Corrupt Practices Act (FCPA), but now this practice is substantially impacted by the newly enacted International Criminal Judicial Assistance Law (ICJAL) in October 2018, which expressly stipulates that institutions, organisations and individuals in China must not provide evidence materials and assistance provided in this law to foreign countries without the consent of the competent authority of China. The ICJAL applies to criminal proceedings with a wide coverage of activities potentially deemed as assisting said crimes. Analysis of different types of FCPA investigations in China indicates that, as long as the investigation could potentially lead to a criminal resolution with the US authorities, the investigation remains within the zone of danger; further, the likelihood of the applicability of the ICJAL on the current FCPA investigations is substantially high with legal implications to be ascertained. Therefore, it is suggested that companies consult with competent local counsel in advance to access the legitimacy of internal investigations and to properly interact with the relevant Chinese authorities.

### Whistle-blowers

Companies in China are now being exposed to the risks arising from the high frequency of whistle-blower complaints. The right to report crimes and other legal violations by citizens is well established in principle in the laws and regulations, such as the Constitution, the Criminal Procedure Law and the Anti-Unfair Competition Law. Although there is currently no consolidated legal regime to regulate whistle-blowing reports, various authorities have respectively promulgated legislation to regulate whistle-blowing reports against certain misconducts in their domain. For instance, the former China Food and Drug Administration (now the SAMR) promulgated the Measures for Rewarding Whistle-Blowing Reports against Food and Drugs Violations in 2013, which was later revised in 2017 to increase the award amount and clarify the relevant procedures and scope.

In practice, to encourage reporting misconduct, multiple authorities have set up reporting hotlines and online gateways to receive whistle-blowing reports from the public.
For instance, the State Supervisory Commission is now operating an ad hoc online channel and hotline (12388)\(^3\) for receiving whistle-blowing reports against government officials’ duty-related crimes or misconducts either by real name or anonymity (real-name reporting is highly encouraged). The national security authorities also encourage whistle-blowing reports made to the designated online platform and hotline (12339).\(^4\) Similarly, the AMRs at all levels have provided online and offline channels to encourage the public to report leads regarding company misconduct, and the handling procedures and specific timelines are published and well implemented.

With respect to whistle-blowers’ protection, some specific rules, such as the Rules of the Supreme People’s Procuratorate on Protecting the Citizens’ Tip-off Rights, were formulated to provide a comprehensive mechanism from both substantial and procedural levels, and the Supreme People’s Procuratorate, the Ministry of Public Security and the Ministry of Finance jointly issued the Several Provisions on Protecting and Rewarding Whistle-Blowers of Duty Crimes in 2016.

Strict confidentiality is the foundational requirement imposed on the authorities that receive any reporting throughout the handling process. Further, the authorities need to take measures (i.e., restraining the physical access of those being reported to the reporter) to ensure the safety of the reporters and their close relatives whenever necessary. Retaliation towards the whistle-blowers is forbidden, and legal liabilities such as administrative punishment, criminal detention or imprisonment can be imposed.

### III ENFORCEMENT

#### i Corporate liability

Administrative and criminal corporate liabilities are stipulated in the Criminal Law and relevant administrative laws and regulations. For criminal liabilities, among the 469 crimes prescribed by the Criminal Law, there are approximately 150 unit crimes for which a company could be qualified as the perpetrator, and for these unit crimes, a company will be held criminally liable if:

\(a\) a collective decision has been made by the management of the company, or an individual decision by the relevant responsible personnel on behalf of the company, such as the legal representative; and

\(b\) the crime is committed in the name of the company and the illegal proceeds go to the company.

The Criminal Law adopts a dual punishment system for unit crime, which means both the company and the responsible persons are subject to the criminal liabilities with only a few exceptions otherwise prescribed in the Criminal Law.

As for the administrative corporate liabilities, they are derived from the respective administrative laws and regulations, such as the Unfair Competition Law, the Anti-Monopoly Law and the Advertisement Law, covering violations such as commercial bribery, monopoly, company illegal operation and illegal advertising.

\(^3\) See www.12388.gov.cn.

\(^4\) See www.12389.gov.cn.
Notably, for the same misconduct committed by a company, the criminal and administrative regimes are mutually exclusive. The Regulations on the Transfer of Suspected Criminal Cases by Administrative Law Enforcement Agencies promulgated by the State Council in 2001 set the regulatory framework for the conversion between administrative and criminal cases. A series of other regulations have been promulgated in the following years to further address the procedure of conversion. According to these regulations, while investigating an administrative case, if the agency suspects that the case should be prosecuted as a criminal case based on elements such as the monetary amount involved, the specific fact patterns or the consequences, then the case must be transferred to a PSB and the PSB will examine the cases transferred. If criminal fact patterns are identified and the PSB decides to investigate the case for criminal liability, it shall notify the administrative agency that transferred the case in writing. If there is no criminal fact pattern or the facts are insignificant, and the agency decides not to prosecute the case, it will state the reasons, notify the administrative agency and return the case. On the other hand, if a PSB discovers that a case it is investigating should not be criminally prosecuted but there may be administrative liability, it shall transfer the case to the relevant administrative law enforcement agency.

**ii Penalties**

Under the Criminal Law, the only sanction applicable to a company is the monetary penalty, but an individual's liabilities for a unit crime include public surveillance, criminal detention, imprisonment, the monetary penalty, the deprivation of political rights, deportation (in the case of foreign nationals) and even the death penalty.\(^5\)

Penalties for administrative corporate liabilities generally include disciplinary warnings, monetary fines, the confiscation of illegal gains or unlawful property, the suspension of production or business, and the temporary suspension or rescission of a permit or licence.\(^6\) The range of penalties varies. Taking commercial bribery as an example, a fine could range from 100,000 yuan to 3 million yuan, as well as the confiscation of illegal gains and the revocation of the business licence.\(^7\) The amount of illegal gains is calculated based on revenue with the corresponding cost being deducted, which could easily add up to 10 million yuan or more, and therefore, in practice, create a larger concern to companies. Other restrictions, such as being banned from participating in government procurement, might also be imposed depending on the nature and severity of the violations. For example, the National Health Commission has established a recording system, which functions as a blacklist, specifically to track commercial bribery activities committed by pharmaceutical companies during drug procurement. Companies committing commercial bribery will be disqualified or severely disadvantaged in public procurement.

Both criminal and administrative penalties are, in principle, made public through the internet with some exceptions, such as where these cases involve state secrets or trade secrets, the personal information of minors or infringe on an individual's privacy, subject to the discretion of the relevant authorities that issue the penalties. Additionally, companies will be included on the publicly available blacklist administrated by the AMRs under certain circumstances (i.e., if a company has been subject to administrative punishment on three or more occasions within three years for unfair competition or distribution of false

\(^5\) Articles 31, 33, and 34 of the Criminal Law.
\(^6\) Article 8 of the Administrative Punishment Law.
\(^7\) Article 19 of the Unfair Competition Law.
advertisements) pursuant to the Interim Measures for the Administration of the List of Dishonest Enterprises Committing Serious Illegal Activities, and will therefore be subject to stringent supervision by the AMRs and restrictions such as being disqualified for certain commercial transactions or relevant honorary titles for five years.

### iii Compliance programmes

Although there is no regulatory requirement for compliance programmes, many companies in China have already incorporated compliance efforts into their internal control mechanisms to ensure compliance with a variety of laws designed for commercial bribery prevention and detection, anti-monopoly, employment and personal information protection. Specific compliance roles and responsibilities within a company are becoming increasingly prominent.

A practical reason for implementing compliance programmes is mitigating and reducing liability for legal violations. For example, in criminal cases where employees are committing crimes in the name of the company, a well implemented compliance programme is likely to negate the company's involvement and knowledge of the criminal conduct to some extent, and be used to corroborate evidence in the company's favour. Likewise, for administrative violations such as commercial bribery, the AMRs will consider a compliance programme as an important factor in evaluating the company's legal liabilities.

On 2 November 2018, the State-owned Assets Supervision and Administration Commission of the State Council, which is the governing authority for all the state-owned enterprises in China, released compliance guidance for all state-owned enterprises. Although this compliance guidance is mainly applicable to state-owned enterprises, other companies could benefit from using it as a major reference for establishing a solid compliance system. A wider range of compliance issues are identified as the key focuses, including anti-corruption and bribery, and anti-unfair competition. Specific requirements include policymaking, establishing risk identification and response systems, compliance review, strengthening accountability, regular compliance trainings, compliance evaluation and continuous improvements.

### iv Prosecution of individuals

Where there has been a unit crime, persons such as legal representatives, general managers or directors could be charged for the crime by the procuratorate depending on their involvement and substantial knowledge of the charged crime. Law enforcement authorities often pursue individuals for the misconducts committed by a company. For example, in January 2018, the Ministry of Public Security and former China Food and Drug Administration jointly issued the Provisions on Intensifying Law Enforcement Concerning Food and Drug Safety and Fully Implementing the Requirement of Imposing Punishment against All Individuals Held Liable for Food and Drug Violations to emphasise the enforcement on individual liabilities for related violations or crimes.

From another perspective, if an employee is being prosecuted for misconduct related to his or her duty, such as offering bribes to a state functionary in exchange for business opportunities without substantial evidence of the company's involvement, the situation will often get complicated owing to the stakeholders' conflicts of interest. It is likely that the employee will raise the defence that the misconduct was under the instruction, approval or with the knowledge of the company to be acquitted from the individual crime of offering bribes, because the individual criminal liabilities for the unit crime of offering bribes are much lighter compared with the individual crime of offering bribes. If the employee is convicted
for the unit crime as the responsible person for the offence, he or she shall be sentenced
to a fixed-term imprisonment of up to five years or criminal detention, and concurrently
sentenced to a fine. In comparison, if the employee is convicted for the individual crime
of offering bribes, the severest punishment could be life imprisonment with confiscation
of property. Under such circumstances, the company has to provide evidence to prove its
ignorance of the employee's conduct and such bribery is not related to efforts of seeking a
transaction opportunity or competitive advantage for the company. Further, it is important for
the company to demonstrate compliance efforts in preventing employees’ misconduct, such
as the internal control mechanisms in place, trainings regularly provided to the employees
and disciplinary actions imposed on violations, to negate the wilful intent and mitigate the
legal risk exposures for the company.

IV  INTERNATIONAL

i  Extraterritorial jurisdiction

The Criminal Law mainly adopts the principle of territorial jurisdiction over criminal
offences, supplemented by the extraterritorial jurisdiction over the circumstances where the
perpetrator is a Chinese citizen or a foreign national commits a crime against China or a
Chinese citizen. Article 10 of the Criminal Law states that any Chinese citizen who commits
a crime outside the territory of China may still be investigated for his or her criminal liabilities
under Chinese law, even if he or she has already been tried in a foreign country. However, if
he or she has already received criminal punishment in the foreign country, he or she may be
exempted from punishment or given a mitigated punishment. Article 8 further states that the
Criminal Law may be applicable to any foreigner who commits a crime outside the territory
of China against China or against any Chinese citizens, if for that crime this Law prescribes
a minimum punishment of fixed-term imprisonment of not less than three years; however,
this does not apply to a crime that is not punishable according to the laws of the place where
it is committed.

ii  International cooperation

China has been actively promoting international and regional judicial cooperation in
combating crimes relating to cybersecurity, corruption, money laundering, terrorism and
drugs; joined international conventions; and signed bilateral judicial assistance and extradition
treaties. In 2018 alone, China signed extradition treaties and mutual legal assistance treaties
on criminal matters with 16 countries, and the enactment of the ICJAL in 2018 further
established the fundamental framework of international cooperation on criminal justice,
clarifying the required process for China to raise requests to, or accept requests from, foreign
judicial authorities regarding criminal judicial assistance.

Anti-corruption is a priority for China in its international cooperation efforts, as
evidenced by claims of a zero-tolerance approach to corruption, and its work on strengthening
international cooperation with a focus on deterrence should help achieve this goal. On
30 November 2018, the State Supervisory Commission successfully extradition a suspect from
Bulgaria accused of taking bribes, which was also the first time that China extradition a suspect
from the European Union. On 13 November 2018, the State Supervisory Commission and
the Australian Federal Police signed a cooperation memorandum regarding anti-corruption
enforcement. All these efforts demonstrate China’s commitments in international cooperation
to combat corruption.
As was reiterated by China’s President during the Fourth Plenary Session of the Central Commission for Discipline Inspection in January 2020, China needs to be clearly aware of the severity and complexity of combating bribery and corruption, which will be a long-term and arduous process. Because more and more cases are significantly implicated with foreign elements in recently years, China will carry the enforcement of ‘Skynet 2020’ and 2020 will be continuously labelled as the year for combating corruption under the international context.

iii Local law considerations

Under the circumstances where a government investigation involves multiple jurisdictions, conflicting law issues might arise. This is particularly true when a foreign government initiates investigation on conducts occurring in China and attempts to conduct an investigation and collect evidence without the proper approval from the Chinese authorities. The ICJAL clearly prohibits any unauthorised criminal investigation by any means, either directly conducted by the foreign authorities, or collaterally through instructing companies in China to collect evidence through internal investigation.

Restriction on cross-border data transfer is another pitfall of which companies need to be aware. The Cyber Security Law, which was promulgated in 2016 and took effect in 2017, establishes the basic framework of data localisation obligations in China. So far, China has promulgated a series of legislation prohibiting the cross-border transfer of certain categories of data in specific industries, such as healthcare and financial industries, and the general legislation and enforcement trend indicates a more restrictive approach by the Chinese authorities. An additional layer of risk in state secret protection is imposed on highly sensitive industries such as telecommunication and infrastructure, for which cross-border data transfer might constitute the crime of supplying state secrets or intelligence for an organ, organisation or individual outside the territory of China, as any information concerning political sensitivity or national security could be retrospectively labelled as a state secret by the Chinese authorities. An individual’s criminal liabilities for violation are clearly stipulated in the Criminal Law.8

V YEAR IN REVIEW

The year 2019 is the first year after the restructuring of the AMRs at all levels, from multiple bureaucratic and administrative agencies into a fully functioning organisation. Though challenging, AMRs at all levels were still able to accomplish their duties. Published statistics shows that, in 2019, the AMRs have substantially strengthened the anti-monopoly enforcement and launched 103 government investigations, among which 28 cases are related to the monopoly agreements, 15 cases are related to abuse of market dominant position, 24 cases are administrative monopoly, and 36 cases are related to failure of declaring concentration of undertakings. In total, 44 monopoly cases were successfully closed in 2019.

8 Article 111 of the Criminal Law: ‘whoever steals, spies into, buys or unlawfully supplies State secrets or intelligence for an organ, organisation or individual outside the territory of China shall be sentenced to fixed-term imprisonment of not less than five years but not more than 10 years; if the circumstances are especially serious, he shall be sentenced to fixed-term imprisonment of not less than 10 years or life imprisonment; if the circumstances are minor, he shall be sentenced to fixed-term imprisonment of not more than five years, criminal detention, public surveillance or deprivation of political rights.’
and the fines add up to 320 million yuan. The key industries for anti-monopoly enforcement include construction, automobile, public utility, healthcare and other industries related to livelihood economy. In April 2020, the SAMR issued the penalty decisions on abuse of market dominant position committed by three active pharmaceutical ingredients distribution companies, and the fines add up to 325 million yuan.

With respect to securities fraud, in 2019, the CSRC issued 136 administrative punishment decisions, which include 55 insider trading cases, 29 cases of illegal information disclosure, 14 cases of market manipulation, 11 cases of illegal activities of intermediaries, and nine cases of practitioners’ violation of laws and regulations. Other violations involve gatekeepers’ failures to exercise due diligence in asset valuation or audit process. Notably, in one on-site investigation against a publicly listed company in Shenzhen, the employees of the company committed violent conducts towards the investigation officers and received administrative penalties including warnings and administrative detention. The company was later punished by the CSRC for refusing to cooperate with the government investigation. Its actual controller and some other senior executives are now prohibited from access to securities market for 5–10 years.

With respect to anti-money laundering enforcement in 2019, the PBOC has published 468 administrative punishment decisions against 319 entities and the fines add up to 172 million yuan in total. The violations mostly involve failure to fulfil the obligations of identifying customer identity, keeping customer identity information and transaction records, or reporting suspicious transactions. The entities that were punished include banks, credit cooperative unions, securities institutions, insurance companies, payment institutions, and asset management companies, etc. Notably, in the first quarter of 2020, the PBOC has published a series of punishment decisions, and the total fines have already exceeded 160 million yuan, indicating a clear trend that more intensive enforcement actions are expected for the rest of 2020.

VI CONCLUSIONS AND OUTLOOK

Although the covid-19 outbreak has been mostly controlled in China and the majority of public functions have been gradually restored, we would still anticipate correlated and substantial impacts on the government-initiated investigations, gradually emerging throughout the year 2020. Nevertheless, companies in China are still advised to pay close attention to updates and changes in regulatory enforcement trends, establish and operate a well-founded compliance mechanism, and continuously strengthen the compliance status, especially for those high-risk areas including anti-corruption, antimonopoly, anti-money laundering, securities fraud, and data protection, etc. As the regulatory compliance environment in China is generally expected to be more and more restrictive, it is always best practice to expend efforts both proactively in preventing non-compliance issues from happening and reactively in preparing and properly handling potential government investigations.
Chapter 10

ENGLAND AND WALES

Stuart Alford QC, Mair Williams and Harriet Slater

I INTRODUCTION

The law on corporate criminal attribution in England and Wales has historically made it difficult to hold entities to account for the actions of their employees. This, in turn, led to a relatively low prioritisation of corporate investigations, which has been subject to change in the past decade and a half. Driven by developments in certain areas of criminal law, increasingly aggressive enforcement in sectors such as financial services, and increasing public demands for corporate accountability, the nature and scope of corporate investigations has been steadily growing.

Several bodies have responsibility for various aspects of corporate investigations:

a. the Serious Fraud Office (SFO) investigates and prosecutes the most serious cases of fraud and other economic crimes in the United Kingdom (UK). This includes lead-agency responsibility for enforcing the Bribery Act 2010 (BA 2010);3

b. the Competition and Markets Authority (CMA) is the main competition regulator and is responsible for enforcing the Competition Act 1998 (CA 1998), the Enterprise Act 2002 and Articles 101 and 102 of the Treaty on the Functioning of the European Union;4

c. the Financial Conduct Authority (FCA) is both a prosecuting body and the regulator of financial institutions, with responsibility for maintaining the integrity of the UK financial markets, including the investigation of financial sector crimes, such as market abuse and insider dealing;5

d. Her Majesty’s Revenue and Customs (HMRC) investigates tax and revenue-related offences with wide-ranging civil and criminal investigatory powers;6

e. the Office of Financial Sanctions Implementation (OFSI) implements the UK sanctions regime;7

---

1 Stuart Alford QC is a partner and Mair Williams and Harriet Slater are associates at Latham & Watkins. The authors would like to acknowledge the kind assistance of their colleague, Alayna Kenney, in the preparation of this chapter.

2 For instance, the Bribery Act 2010, which introduced a corporate offence of ‘failure to prevent bribery’.

3 The SFO was created by and derives its investigatory powers from the Criminal Justice Act 1987 (CJA), which include powers to request the production of documents and the answering of questions.

4 The CMA’s powers are largely drawn from the CA 1998 itself.

5 The FCA’s investigatory powers are derived from the Financial Services and Markets Act 2000.

6 HMRC’s investigatory powers are derived from the Finance Act 2009 (civil) and the Police and Criminal Evidence Act 1984 (criminal).

7 The OFSI’s powers come from the Policing and Crime Act 2017.
the Crown Prosecution Service (CPS) prosecutes cases investigated by the police forces of England and Wales, as well as on behalf of HMRC and the CMA (which have only investigatory powers and no prosecuting authority); and

the National Crime Agency (NCA), which includes the National Economic Crime Centre (NECC), coordinates and assists the work of the other agencies and the police in the investigation and prosecution of economic crime.

These bodies have distinct remits, albeit with some overlap, and a range of powers to enforce the legislation within those remits. This includes the ability to execute search warrants and to file compulsory production notices for the production of documents in certain cases. Some of these powers can only be exercised with a court order, some have to be exercised with the assistance of the police, and others are wholly in the control of the agency themselves (determined by the statutory powers by which they are established).

The ability and extent of the powers to obtain material has been the subject of a number of important challenges through the courts in recent years, which will be discussed further below. Corporations are not permitted to withhold documents from the authorities on the grounds of client confidentiality and data privacy, and must hand over any materials requested by such notices and orders, save when legal privilege applies. It is a separate criminal offence in England and Wales not to comply with a lawful production order.

Another area of significant development in the law has been the introduction of deferred prosecution agreements (DPAs), which are available to prosecutors in both the CPS and the SFO. Under a DPA, corporations accused of certain criminal offences are permitted to enter into an agreement with the prosecutor to defer a prosecution (and, potentially, avoid a prosecution altogether) if they fulfil the terms of an agreement approved by a judge. The agreement usually includes payment of a financial penalty, costs and compensation; implementation of, or improvement to, a compliance programme; and cooperation with ongoing investigations. So far, there have been seven DPAs in the UK, including three in the 2019/2020 financial year, a considerable increase from previous years, although the regime has come under considerable criticism (see Section III.iv).

II CONDUCT

i Self-reporting

A corporate’s approach to self-reporting in England and Wales must be considered against a broad spectrum of factors, which include the nature of the issue, the prospect of enforcement activity, the benefits of cooperation with authorities, the industry sector in which the corporate operates and the supervisory regime applicable to the corporate. Although there is no obligation to self-report most criminal conduct, there are notable exceptions for

---

8 The prosecuting powers of the CPS (and the SFO and FCA) are governed by the Code for Crown Prosecutors, which was updated in 2018 (available at: www.cps.gov.uk/sites/default/files/documents/publications/Code-for-Crown-Prosecutors-October-2018.pdf).

9 The National Crime Agency was created by the Crime and Courts Act 2013. The NECC started operations on 31 October 2018.

10 The law of privilege in England and Wales has been the subject of a number of court challenges in recent years (see Section IV.iii).

11 DPAs are not available for individuals.
those operating in regulated sectors such as financial services. The decision of whether to self-report will need to take into account this wide range of factors, as well as the possibility of enforcement actions in other jurisdictions (which will be subject to their own decision in respect of self-reporting) and will usually be taken with the assistance of legal counsel.

The FCA’s principles of openness create an expectation that the entities they regulate will self-report issues. The regulator has regularly made clear that it regards self-reporting to be a key part of the open and cooperative relationship it expects of its regulated entities. Within its guidance, the FCA mandates a large number of reporting requirements including reporting in relation to complaints, accounts and market abuse. The principle of openness has, on several occasions, been the basis for fining firms for failing to adequately self-report.

The CMA operates a more discretionary approach to self-reporting, but one based on an explicit framework for the recognition of reporting. The leniency programme is designed to encourage companies that have been involved in wrongdoing to proactively cooperate with the CMA. To encourage self-reporting, the CMA offers a sliding scale of leniency ranging from total immunity to reduced financial penalties, depending on the timing of the self-reporting. As with most self-reporting regimes, the earlier the report is made, the more lenient the authority will be.

Although not as structured as the CMA scheme, a similar incentive-based self-reporting principle is operated by the SFO and CPS. The SFO’s policy on corporate self-reporting states that self-reporting will be a key factor in deciding whether to prosecute. On 6 August 2019, the SFO published new Corporate Co-operation Guidance that outlines cooperative steps companies can take to gain credit from the SFO, which it will take into account when deciding whether to issue a charging decision, DPA or other appropriate sanction, if at all. The benefits of self-reporting have also been highlighted in the guidance provided for DPAs. Initially the SFO had indicated that only companies that self-reported would be eligible for a DPA, but both Rolls-Royce and Tesco have been able to secure DPAs without self-reporting. Self-reporting has played an instrumental role in all of the DPAs agreed in the 2019/2020 financial year; for example, the SFO Director, Lisa Osofsky, stated that the DPA agreed with

---

16 MAR Schedule 2, the FCA Handbook (available at: www.handbook.fca.org.uk/handbook/MAR/ Sch/2/2.html).
17 OFT and CMA Penalty Guidance and criminal immunity provided by Section 190(4) of the Enterprise Act 2002.
22 It was noted that without self-reporting, Rolls-Royce was only considered for a DPA because of its ‘exemplary’ cooperation (available at: https://globalinvestigationsreview.com/article/1138835/self-reporting-after-rolls-royce-is-it-worth-it).
Güralp Systems Limited was because of its ‘timely self-reporting and full cooperation’.\textsuperscript{23} In the non-regulated sectors, the decision as to whether to self-report is a balance between a number of incentives and disincentives that require careful consideration.

An additional but discrete layer of strict self-reporting is required under the Proceeds of Crime Act 2002 (POCA 2002). POCA 2002 legislates for a number of criminal money laundering offences, including becoming concerned in an arrangement that the person knows or suspects facilitating the acquisition, retention, use or control of criminal property by or on behalf of another person.\textsuperscript{24} Voluntary self-reporting through an authorised disclosure may be used as a defence to such an offence.\textsuperscript{25} Although self-reporting is not compulsory for non-regulated persons, it is a criminal offence for a regulated person – who has reasonable grounds for knowing or suspecting that another person is engaged in money laundering – to fail to report such knowledge or suspicion.

\textbf{ii Internal investigations}

Internal investigations are increasingly used by both international and domestic companies as a way of mitigating risk as well as honouring regulatory obligations. It is no longer a viable option for a company to turn a blind eye to any allegations or suspicions that it receives about its business operations, and an internal investigation is a common first step in dealing with potential issues.

Preliminary or scoping interviews occur in the very early stages of investigations and are used to identify useful information and where further evidence might be located. Witness interviews form a crucial part of internal investigations. Importantly, these interviews may take place on the understanding – between the interviewer and the employee – that they are confidential and attract privilege.\textsuperscript{26} However, ‘the law as it stands today is settled. Privilege does not apply to first interview notes’: unless those notes contain privileged legal advice, when privilege would then apply.\textsuperscript{27}

Authorities expect details of witness interviews to be provided to them. This expectation is set out in the form of speeches and guidelines as opposed to law. To gain the benefit of a DPA, the SFO has said it expects companies to cooperate and comply with Clause 2.8.2(i) of the Code of Practice on Deferred Prosecution Agreements (the DPA Code) by ‘identifying relevant witnesses, disclosing their accounts and the documents shown to them and, ‘where practicable’, making witnesses available for interview when requested’.\textsuperscript{28}

The SFO has not set out clear guidance as to the detail it expects to be provided with witness interviews;\textsuperscript{29} however, it has made it clear that ‘first accounts’ are expected as part of any information given to the SFO. There does not appear to be a consistent practice

\begin{footnotes}
\item[24] Section 328(1), POCA 2002.
\item[25] e.g., Section 328(1), POCA 2002.
\item[27] R (on the application of AL) v. Serious Fraud Office [2018] EWHC 856 (Admin).
\end{footnotes}
in this regard, and the approach can vary case-by-case. Over the past five years, there has been a suggestion from the SFO that they are reluctant to see companies conducting internal investigations for fear of them ‘trampling the crime scene’. Under the current SFO Director, however, there appears to have been a shift in this approach. For example, in its Corporate Co-operation Guidance, the SFO stipulates that for a company to be considered cooperative it should, among other things, provide the evidence that is has collected during an internal investigation.

The FCA also takes a cautious approach to internal investigations and has noted a number of potential issues with internal investigations. These issues include poor communication with the FCA at the early stages of an investigation resulting in a report that is unhelpful for FCA purposes, or even the risk that a subsequent FCA investigation is prejudiced or hindered by a firm’s own internal investigation.

By contrast, the CMA’s approach to self-reporting necessitates internal investigations, in particular the requirement for supporting evidence in claims for leniency; however, these internal investigations are required to be limited to what is strictly necessary to minimise the risk of ‘tipping off’ other parties to cartel activity. As part of the leniency application process, companies are required to take ‘careful note’ of all investigative actions and keep records until the conclusion of any related proceedings.

One issue related to internal investigations that has received significant attention in the past few years is legal professional privilege. In England and Wales, internal legal counsel attract the same legal privilege as external counsel, so one of the advantages of instructing external counsel may not exist compared to other jurisdictions. The extent of that privilege has been the subject of judicial decision in *Director of the SFO v. Eurasian Natural Resources Corporation Limited* [2018] EWCA Civ 2006 (ENRC), where the Court of Appeal reversed the first-instance decision in which the High Court agreed with the SFO’s view that litigation and legal advice privilege did not apply in the context of documents that were generated during an investigation by forensic accountants and lawyers (see Section IV.iii).

In most internal investigations, employees will not receive their own independent legal advice. This is because the interviews are simply part of a fact-finding investigation and the employee is not treated as a suspect. In these circumstances, cooperation between employees and their companies will be in both parties’ shared interests. At the outset of any fact-finding interview, the individual must be advised that the lawyers representing him or her are the company’s lawyers and that the company holds the privilege.

However, in some circumstances, independent legal representation for the employee may be either necessary or desirable; for example, if the employee is a suspect, or risks incriminating themselves or admitting regulatory breaches, or has the potential to create

---

30 Speech by Alun Milford, then SFO General Counsel, at GIR London Live, on 27 April 2017 (reported by GIR on 27 April 2017) and Speech by Alun Milford, then SFO General Counsel, at the Cambridge Symposium on Economic Crime 2017, Jesus College, Cambridge.

31 ibid., and interview with *The Times*, published 27 August 2014, David Green QC, then director of the SFO (available at: www.thetimes.co.uk/article/fraud-office-attacks-flawed-crime-reports-jj6x827q5c6).

32 Lisa Osofsky took up the role of SFO director on 28 August 2018.


35 id., at p. 32.

36 *Director of the SFO v. Eurasian Natural Resources Corporation Ltd* [2017] EWHC 1017 QB.

37 Similar to an Upjohn warning given in the United States.
a liability for the employer. In these circumstances, there may be a conflict between the best interests of the employee and their employer and independent legal advice would be appropriate.

iii Whistle-blowers

There is market-wide protection for whistle-blowers set out in the Public Interest Disclosure Act 1998 (PIDA 1998). PIDA 1998 has a significantly broader definition of ‘worker’ than the Employment Rights Act 1996, which includes employees, employee shareholders and agency workers.\(^{39}\) Should an employer dismiss a worker for the reason (or principal reason) that the employee made a ‘protected disclosure’, this dismissal will automatically be unfair. Further, if an employer subjects an employee to any detriment for reason that he or she made a protected disclosure then they could also have a distinct claim for detriment up to the date the employee was dismissed. Detriment can include damaged career prospects, dock of pay or loss of work and disciplinary action. The tests for qualifying for protection are:\(^{40}\)

\begin{enumerate}[a]
  \item Was the disclosure a qualifying disclosure?
  \item Has the worker made a disclosure of information?
  \item Did the subject matter of the disclosure relate to one of the types of ‘relevant failure’?
  \item Did the worker have a reasonable belief that the information shows that one of the six relevant behaviours has occurred?
  \item Did the worker have a reasonable belief that the disclosure was in the public interest (not applicable to disclosures made before 25 June 2013)\(^{41}\)
  \item Was the disclosure a protected disclosure?
\end{enumerate}

In March 2019, the former Prime Minister Theresa May announced that the government would be bringing in changes to the operation of non-disclosure agreements, particularly those that operate between employees and employers. One of the stated motivations for the changes is to give whistle-blowers additional protections and to ensure individuals are not put off from reporting their concerns to the appropriate enforcement agencies. There have not, to date, been any legislative changes on the back of this announcement.

On 8 September 2019, the Council of Ministers adopted the EU Whistleblower Directive (the Directive) which grants greater protections to individuals who report any breach of EU law. While the Directive is to be treated as a floor for unified protections across the EU, countries can further strengthen their own regimes as they wish. Given the UK’s departure from the European Union (EU) on 31 January 2020, the applicability of the Directive after the UK’s transition period is uncertain and, at the time of writing, the UK is not going to implement the Directive. However, the proposals prior to the implementation of the

---

\(^{38}\) This section deals with workplace-based whistle-blowing. The UK Code of Practice for Victims of Crime and the Witness Charter provides protection outside the context of the workplace for whistle-blowers.

\(^{39}\) Section 43K(1)(a)(iii) PIDA 1998.


\(^{41}\) Since June 2013, the disclosures no longer need to be made in good faith in order to be protected.
Directive noted that the UK was one of the Member States that already has a comprehensive regime in place and many of the protections underpinning the Directive already exist in legislation such as PIDA 1998.

The financial services sector has developed a more rigorous whistle-blower regime than that created under the PIDA 1998. The current regime applies to around 8,000 companies operating in the financial services sector, but it is estimated that this could increase to 55,000 companies once the regime is widened. The FCA has reported that whistle-blowing ‘is on the rise’ and that it investigated 1,119 whistle-blower complaints in 2019 alone.

On 14 November 2018, the FCA published its research into the consequences of the new whistle-blowing rules introduced on 7 September 2016. These rules can be found in the Senior Management Arrangements Systems and Controls and they require firms to:

- have effective arrangements in place for employees to raise concerns, and to ensure these concerns are handled appropriately and confidentially. The requirement to appoint a whistle-blowers’ champion is to ensure there is senior management oversight over the integrity, independence and effectiveness of the firm’s arrangements.

The Financial Reporting Council (FRC), which is responsible for setting UK standards of corporate governance, includes, within the UK Corporate Governance Code 2018, a principle that ‘[t]here should be a means for the workforce to raise concerns in confidence and – if they wish – anonymously’. This code, however, operates on a ‘comply or explain’ basis, so listed companies are not obliged to have a whistle-blowing policy in place, even if it is good practice.

Similarly, the Ministry of Justice (MOJ) suggests that having adequate whistle-blowing procedures may be an important part of asserting an ‘adequate procedures’ defence to the offence of failing to prevent bribery under Section 7 BA 2010 and the British Standards Institution outlines whistle-blowing procedures as part of its published standard for Anti-Bribery Management Systems.

In contrast to the system used by the Securities Exchange Commission in the United States (US), there are currently no monetary incentives in England and Wales for whistle-blowers to come forward, and the Directive also does not require them. The Home Office has previously considered introducing financial incentives for whistle-blowers who

47 The FRC regulates the audit industry in the UK.
48 www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.pdf (1(6)).
49 Ministry of Justice Guidance about procedures that relevant commercial organisations can put into place to prevent persons associated with them from bribing, at Paragraph 1.7.
come forward on matters of ‘fraud, bribery and corruption’; however, research from various groups, including the FCA and the Prudential Regulatory Authority (PRA), concluded that providing financial ‘incentives’ would not in fact encourage whistle-blowing.

III ENFORCEMENT

i Corporate liability

The case law on corporate civil liability is voluminous. In general, a corporate employer is vicariously liable for the acts of its employees if it would be fair and just to hold the employer vicariously liable. If the employees’ acts are within the ordinary course of their employment, this will usually be sufficient.

By contrast, corporate criminal liability is normally only relevant if a criminal offence imposes strict liability and the state of mind of the company (acting through its employee) does not need to be established. In addition, there are a growing number of statutory offences that create a corporate liability, such as the offence of ‘failing to prevent bribery’ under Section 7 of the BA 2010, which is discussed further below.

Apart from those offences that create a direct corporate liability, companies will only be liable for offences requiring proof of a criminal state of mind by application of the ‘identification principle’. The identification principle imputes, to the company, the acts and state of mind of the individuals who represent the ‘directing mind and will’ of the company. This is much more narrow than the basis of attribution in the US, for instance, where a company can be liable for the actions of its agents and employees when they act within the scope of their employment and, at least in part, to benefit the company (which is more akin to the basis for civil liability in England and Wales).

The leading case of Tesco Supermarkets v. Nattrass [1972] AC 153 defines the ‘directing mind and will’ of the company as the directors and, in certain circumstances, other senior officers of the company who carry out management functions and speak and act as the company. The test of attribution may also be met if the directors have delegated part of their management functions. This has historically been very difficult to prove against companies and this has only got more difficult as complex corporate structures become a common feature in UK corporate bodies.

The BA 2010 introduced a new approach to establishing corporate criminal liability in the UK. It legislates for bribery offences committed in the UK and abroad by individuals and companies. Section 7 of the BA 2010 creates the offence of ‘failure to prevent bribery’, which can be committed by a corporate entity only. It first requires that a person associated with the company has committed an offence under Sections 1 or 6 of the BA 2010 or would have done if they were within the territorial scope of the BA 2010. A person is ‘associated with’ the company if they perform services for or on behalf of the organisation in any capacity. This is, therefore, not confined to employees but also covers agents such as independent contractors.

Second, Section 7 of the BA 2010 requires that the person who committed the offence to have intended either to obtain or retain business or an advantage in the conduct of business.

---

53 Certain statutory offences may refine the general common law rule and specify different rules of attribution or require a different application of the rules in a particular case.
for the company. Knowledge on behalf of the company is not required. Section 7 of the BA 2010 has a broad territorial scope and applies not only to UK-incorporated companies but also those that carry on a business or part of a business in the UK.

It is a complete defence to the corporate offence of ‘failure to prevent bribery’ that the company had in place ‘adequate procedures’ to prevent acts of bribery by persons associated with it (this is discussed in more detail below).

ii Penalties

The approach to sanctions against businesses for corporate misconduct has shifted in recent years. Corporations considered liable of corporate misconduct can suffer penalties ranging from a minor fine to a substantial financial penalty and severe criminal consequences from a selection of prosecuting bodies.

The Financial Services and Markets Act 2000 (FSMA 2000) grants the FCA the power to impose a variety of sanctions ranging from public censure to the revocation of FCA authorisations and large regulatory fines.54 There were a number of notable fines associated with breaches of the FCA’s Principles for Business in 2019.55 Carphone Warehouse, for example, was fined £29,107,600 for mis-selling a mobile phone insurance and technical support product.56 FSMA 2000 also grants the FCA the power to bring criminal prosecutions for the purpose of tackling financial crime such as investigations for insider dealing pursuant to the Criminal Justice Act 1993, and breaches of the recently enacted Sanctions and Anti-Money Laundering Act 2018. The FCA’s Decision Procedure and Penalties Manual sets out a non-exhaustive list of the factors that the FCA considers before issuing a penalty, which includes looking at the nature, seriousness and impact of the suspected breach, the conduct after the breach and previous disciplinary record and the compliance history of the person in question. The FCA will also consider ‘the full circumstances of each case’ when determining whether to impose a penalty.57

The CMA also has a range of criminal and civil powers afforded to it under legislation with regard to competition law infringements. The CMA can impose fines for breach of the CA 1998 if the CMA is satisfied an infringement has either been intentionally or negligently committed.58 The most notable fine that the CMA can impose is an amount of up to 10 per cent of a firm’s worldwide turnover in the business year that proceeds the date of the CMA’s decision.59

The CMA can also impose settlement and the making of commitments.60 Settlement allows early resolution of investigations by way of a voluntary process if a business under investigation by the CMA for a breach of competition law admits a breach and accepts a streamlined version of the process that will govern the remainder of the CMA investigation. In return for its cooperation and an admission of wrongdoing, the business will gain a

---

54 See FSMA 2000.
56 ibid.
58 CA 1998.
60 Sections 31E and 34 of the CA 1998.
reduction in any financial penalty that the CMA imposes. Commitments and directions in relation to the settlement are agreed between the CMA and the firm and the courts have the power to enforce them in the event of non-compliance.

The SFO has the power to prosecute in cases involving serious or complex fraud, bribery and corruption. Alternatively, the SFO may consider inviting a company to enter into a DPA. DPAs were introduced in the UK in 2014 as a discretionary tool for use by the SFO that enables prosecutors to enter into agreements with the offending corporation to suspend prosecution for a defined period of time so long as specified conditions are met by the business during the suspension period.\(^6^1\) DPAs are supervised by a judge and governed by the DPA Code published by the SFO and the CPS, which states that the SFO’s role is as a prosecutorial authority and that DPAs are for use only in exceptional circumstances.\(^6^2\)

Corporate tax offences are resolved primarily by means of a civil resolution by HMRC. It is also possible that corporate tax offences can lead to criminal charges in the circumstances of corruption or links to wider criminal offences either in the UK or overseas.

If a corporation breaches any UK or international sanction, a distinct Treasury unit, the OFSI, is the competent authority for the implementation of penalties, including financial penalties under the Policing and Crime Act 2017. The maximum penalty that the OFSI can impose will be the greater of £1 million or 50 per cent of the value of the breach.\(^6^3\)

Individuals prosecuted by these agencies can be ordered to pay fines, compensation and court costs and may receive prison sentences if the offences are serious enough. In addition, individuals may be disqualified from holding directorships in the UK.

### iii Compliance programmes

Both the CMA and the FCA publish a variety of documents to assist companies in meeting their compliance obligations, including annual plans and a great deal of guidance in the run up to the UK’s planned departure from the EU.

As described above, the BA 2010 provides a defence to the Section 7 offence, if a commercial organisation can show on the balance of probabilities that it had in place ‘adequate procedures’ designed to prevent bribery. The MOJ has provided guidance on what constitutes ‘adequate procedures’ for the purposes of the defence, including six principles to provide businesses with guidance in establishing and maintaining a compliant anti-bribery regime. The principles are:

- **a** proportionate procedures;
- **b** top-level commitment;
- **c** risk assessment;
- **d** due diligence;
- **e** communication; and
- **f** monitoring and review.\(^6^4\)

---


The guidance is clear that it is not enough for a company to have a suite of policies, the culture of compliance and regular training will also be an important part of determining whether procedures will be considered adequate.

The BA 2010 ‘adequate procedures’ defence was tested for the first time in the case of **R v. Skansen Interiors Limited** (unreported). The case concerned two bribes that had been paid to an employee managing the tender for an office refurbishment by Skansen Interiors Limited (SIL), a small refurbishment company. When a new chief executive officer took over at SIL and learned about the payments that had been made, he initiated an internal investigation and established an anti-bribery and corruption policy. SIL then submitted a suspicious activity report to the NCA.

The question for the jury was whether SIL had adequate procedures in place. SIL argued, inter alia, that: its policies and procedures were proportionate to its size – it was a very small business operating out of a single open-plan office; its business was very localised, removing the need for more sophisticated controls; it was ‘common sense’ that employees should not pay bribes; the ethos of the company was one of honesty and integrity; and a company of its size did not need a more formal policy. The jury did not agree and returned a guilty verdict.

A similar offence to the Section 7 of the BA 2010 offence exists in Sections 44 and 45 of the Criminal Finances Act 2017 (CFA 2017) in relation to the failure by a company to prevent a tax evasion offence by an associated person, which include a similar ‘reasonable procedures’ defence.

### iv Prosecution of individuals

The CPS and the SFO look to prosecute individuals for financial crime; when a business is prosecuted within England and Wales, enforcement action will usually also be taken against individuals involved. Guidance states that the prosecution of a company should not be seen as a substitute for the prosecution of criminally culpable individuals such as directors, officers, employees or shareholders of the offending company. The prosecution of individuals in circumstances involving corporate misconduct is viewed as essential in providing a strong deterrent against future corporate wrongdoing.

When proceedings or enforcement action is launched against individuals, the company involved must be conscious of its obligations towards its employees. Often, corporates will suspend the individuals suspected of wrongdoing for the duration of any investigations; however, any suspension must be deemed to be fair and reasonable. Individual employees may be entitled to further assistance from their employer company by means of assistance with legal fees in the event of any investigations, although there is no statutory requirement for this currently. Alternatively, some employees may be entitled to some form of officer liability insurance, which can provide cover for the duration of any investigations or trial. Given the scale and cost of government investigations to date, this has become the norm in larger companies.

Recently there has been attention on the SFO’s failure to prosecute individuals connected to corporations who are the subject of criminal proceedings. In February 2019, two years after the Rolls-Royce DPA was secured (with the company paying £497.25 million),

---


66 ibid.
Lisa Osofsky announced that senior employees from the company would not be prosecuted because of ‘insufficient evidence’ and because such a prosecution was ‘not in the public interest’.

Similarly, in December 2019, two months after the SFO confirmed a DPA with Güralp Systems Limited, its founder and two former employees were acquitted of charges of conspiring to bribe public officials. In December 2019, the SFO charged two former directors of Serco Geografix Limited, which had entered into a DPA with the SFO in July 2019, but these former directors are yet to be tried. This means that the SFO has so far failed to prosecute any individuals associated with the DPAs it has entered into.

In December 2018, the trial of three former executives from Tesco collapsed, with Sir John Royce, the judge in the last of these Tesco trials, going so far as to say that ‘the prosecution case was so weak that it should not be left for a jury’s consideration’. There has been criticism that the statement of facts entered into by Tesco, in its DPA with the SFO, can assert that the three former executives were ‘aware of and dishonestly perpetuated the misstatement [of figures] . . . thereby falsifying or concurring in the falsification of accounts or records’ and yet, when these assertions are tested in criminal court, they collapse, leaving the individuals with limited options for relief or recourse. The lawyers who defended John Scouler, former food commercial director at Tesco, noted: ‘despite his acquittal, Mr Scouler finds himself labelled as culpable in a private agreement, but one which is now made public, which the SFO concluded with Tesco before the SFO’s evidence was heard’. It remains to be seen how the SFO considers the need for actual convictions as part of the consideration for granting a DPA in the future.

Although there have not been any successful prosecutions of individuals associated with DPAs, the SFO has been successful in prosecuting some individuals, most notably in connection with London Interbank Offered Rate (LIBOR) or Euro Interbank Offered Rate (EURIBOR) rigging. For example, on 4 March 2020, the SFO secured the conviction and imprisonment of former bankers for manipulating EURIBOR. The former bankers also faced a fine for £1.2 million. The SFO recently concluded its long-running investigation into the LIBOR/EURIBOR scandal.

While there has been an increasing interest in the ability of the authorities to pursue cases against companies, the prosecution of individuals has continued to represent the greater part of the prosecutor’s activities, including significant financial penalties and prison sentences. Legislative changes have made it easier for the authorities in the UK to prosecute companies, but these authorities all remain committed to the investigation and punishment of individuals.

71 Tesco bosses’ trial collapse puts plea bargain in dock; Retail & consumer. Courtroom drama Chain criticised for ‘throwing executives under the bus’ over accounting scandal’, Financial Times (Jane Croft and Jonathan Eley), 24 January 2019, p. 17, www.ft.com/content/b6c2b688-1f29-11e9-b126-46fc3ad87c65.70.
72 www.sfo.gov.uk/2020/03/05/euribor-bankers-ordered-to-pay-over-1-2-million/.
IV INTERNATIONAL

i Extraterritorial jurisdiction

Any departure from the general presumption against the creation of extra-territorial liability must be expressly provided by the legislature;\(^\text{73}\) below is an overview of key examples of pieces of UK legislation containing corporate offence provisions with extra-territorial reach.

The BA 2010 has a wide territorial remit, covering offences that take place in the UK or overseas as long as the company is either UK incorporated or carries on a part of its business in the UK.\(^\text{74}\)

Among other laws, POCA 2002 contains the UK’s money laundering offences. Broadly speaking, the money laundering provisions aim to tackle the channels through which proceeds of criminal activity pass. In terms of jurisdictional reach, the location of the underlying criminal conduct is irrelevant; if the conduct would amount to a criminal offence in the UK, had it occurred there, then it will fall within the ambit of POCA 2002, subject to very limited exceptions.\(^\text{75}\) In addition, UK nationals, living overseas, can also be prosecuted for money laundering offences committed outside the UK.

The offence of failure to prevent the facilitation of tax evasion was introduced by the CFA 2017 and applies to both domestic and overseas tax evasion. Under the CFA 2017, companies are liable for the conduct of their associated persons who facilitate the evasion of either UK or overseas tax. For the UK tax evasion offence, the conduct can occur anywhere in the world; for the foreign tax evasion offence, the relevant body must either be incorporated in the UK, carry on business in the UK or the relevant conduct must have taken place in the UK. ‘Relevant bodies’ will be liable for failing to prevent the actions of their employees and other associated persons who criminally facilitate tax evasion.\(^\text{76}\) A ‘relevant body’ is a company or partnership, irrespective of jurisdiction of incorporation or formation.\(^\text{77}\) A ‘person associated’ with the relevant body is an employee, an agent or any other person performing services for or on behalf of that relevant body.\(^\text{78}\) To the extent the offence took place outside the jurisdiction, UK prosecutors need to prove, to the criminal standard, that both the taxpayer and the associated person committed an offence. Like the corporate offence under the BA 2010, the CFA 2017 provides companies with a defence where they can show that they had in place ‘reasonable procedures’ to prevent the offending.

With the increase of online criminal activity, the Crime (Overseas Production Orders) Act 2019, which came into force on 12 February 2019, will provide a useful basis for investigators and prosecutors that require quick access to electronic data (such as emails).

\(^{73}\) ibid.

\(^{74}\) Section 7 of the BA 2010 applies to any ‘relevant commercial organisation’ that Section 7(5) of the BA 2010 defines as:

\(a\) a body incorporated under the law of any part of the UK and that carries on a business (whether there or elsewhere), or any other body corporate (wherever incorporated) that carries on a business, or part of a business, in any part of the UK; or

\(b\) a partnership formed under the law of any part of the UK and that carries on a business (whether there or elsewhere), or any other partnership (wherever formed) that carries on a business, or part of a business, in any part of the UK.

\(^{75}\) As confirmed by \(R v. Rogers [2014] EWCA Crim 1680\).


\(^{77}\) Sections 44(2) and (3) of the CFA 2017.

\(^{78}\) Section 44(4) of the CFA 2017.
situated outside the UK. However, the extra-territorial power will only be effective when there is a cooperation agreement in place between the UK and the jurisdiction where the holder of the data is located. At the time of writing, there is only one cooperation agreement in place which is between the UK, Northern Ireland and the US.79

ii International cooperation
The UK authorities work with their counterpart authorities in other jurisdictions in a variety of ways. Some ‘formal’ methods of cooperation are set out below, but it is not uncommon for international enforcement authorities to share information with their foreign counterparts through more informal channels of communication, relying on established relationships.80

Following the UK’s exit from the EU on 31 January 2020, there is a degree of uncertainty regarding the future framework for international cooperation between the UK and Europe. Presently and during the UK’s transition period (which is currently expected to last until 31 December 2020) the current framework remains in force, but it is not clear how negotiations will affect mechanisms for European cooperation and what will happen to the UK’s access to EU criminal data bases and the operation of the European Arrest Warrant.

The UK has a number of statutorily created ‘information gateways’ that enable certain authorities to share and supply information with each other, internationally and domestically. For instance, Section 68 of the Serious Crime Act 2015 permits public authorities to disclose information to other organisations to prevent fraud. Part XXIII of the FSMA 2000 allows for disclosure of information to enable the performance of a public function, and Part 9 of the Enterprise Act 2002 allows for the disclosure of information received by the CMA in certain circumstances, such as where it is disclosing that information to another authority for the purposes of criminal proceedings.

Typically, authorities may enter into memorandums of understanding (MOUs) with domestic and overseas authorities that have a similar remit. MOUs tend to explicitly set out available gateways that may be relied on and provide guidance as to how the information is transferred. For example, the PRA and FCA have entered into a number of MOUs with equivalent authorities in other jurisdictions, such as the MOU between the Dubai Financial Services Authority and the PRA, dated 12 June 2014,81 and the MOU between the US Commodity Futures Trading Commission and the FCA, dated 6 October 2016.82

Multilateral and bilateral mutual legal assistance (MLA) treaties are a form of cooperation between different countries that allow for the collecting and exchanging of information.83 Authorities may request and provide evidence located in one country to assist in criminal proceedings or investigations in another.84 The UK has signed a number of multilateral and

84 ibid.
bilateral MLA treaties, such as the bilateral agreement with the US in 1994. Cross-border criminal investigations often involve suspects that reside outside the jurisdiction in which the investigation is being conducted. UK extradition is governed by the EU Framework Decision, implemented through the Extradition Act 2003. In the UK there are two forms of extradition: export extradition, which relates to a request by another state for the extradition of someone from the UK; and import extradition, which relates to a request to another state for the extradition of a person to the UK.

A number of bars to extradition exist, including the ‘forum bar’, which provides that extradition may be barred if it would not be in the interests of justice.

iii Local law considerations

Data privacy

The UK remains subject to the EU’s General Data Protection Regulation (GDPR) until 1 January 2021. The GDPR has extra-territorial application to organisations that monitor behaviour of individuals that takes place within the EU, or to organisations offering services or goods to individuals in the EU. The government of the UK has issued its own version of the GDPR, namely the United Kingdom General Data Protection Regulation (the UK-GDPR), which took effect on 31 January 2020, and does not contain any significant differences to the GDPR.

The GDPR imposes strict data protection obligations and prohibits the transfer of personal data from the UK to a location outside the European Economic Area (EEA) unless the recipient, jurisdiction or territory is able to ensure a UK-equivalent level of protection. As it stands, the European Commission has determined that only a few countries provide ‘adequate’ levels of protection, while many other countries, such as the US, fall short of the standard. This means organisations operating in the UK may be limited in their ability to transfer personal data into various non-EEA territories.

July 2016 saw the adoption of the EU–US privacy shield adequacy decision (the Privacy Shield). The Privacy Shield requires US companies to protect EU citizens’ personal data in accordance with particular standards; for instance, limiting the conditions for onward transfer of data to third parties, as well as transparency obligations on access by the US government. However, a recent review carried out by the European Data Protection Board (EDPB) noted that areas requiring significant improvement remain, which the EDPB considers both the

---

86 2002/584/JHA.
88 Parts 1 and 2 respectively of the Extradition Act 2003.
89 Sections 19B (Part 1 cases) and 83A (Part 2 cases), Extradition Act 2003; not in force in Scotland.
91 The United Kingdom General Data Protection Regulation.
94 ibid.
Commission and US authorities should address.\(^{95}\) Particular areas of concern include the
absence of substantial checks, the application of Privacy Shield requirements regarding
onward transfers and human resources data and processors.\(^{96}\)

**Legal professional privilege**

Legal professional privilege has been a heavily litigated issue in recent years. England and
Wales recognises two forms of legal professional privilege, in respect of both in-house and
external counsel:

\(a\) ‘litigation privilege’, which attaches to communications passing between a lawyer
and a client, and also between a lawyer or client and a third party (such as a forensic
accountant), for the sole or dominant purpose of preparing for adversarial litigation.\(^{97}\)
The litigation can either be in progress or in contemplation, and includes civil and
criminal litigation; and

\(b\) ‘legal advice privilege’, which attaches to confidential communications passing between
lawyer and a client for the purposes of giving or receiving legal advice. It will not
usually apply to communications between a company and its own employees in the
context of an investigation.

The meaning of ‘client’ was discussed in detail in *Three Rivers No. 5* [2003] EWCA Civ 474,
yet the ratio of the case has been inconsistently understood and, although it has been recently
criticised,\(^{99}\) *Three Rivers No. 5* remains the leading authority in this respect. The concept of
‘client’ in a corporate context was considered again in *The RBS Rights Issue Litigation*, in
which Hildyard J held that interview notes produced by lawyers during the course of an
internal investigation were not protected by legal advice privilege.\(^{100}\) Hildyard J understood
the *Three Rivers No. 5* decision as establishing the principle that the ‘client’, for the purposes
of a lawyer–client communication protected as legal advice privilege, must be someone who
is authorised to seek and receive legal advice.\(^{101}\)

This approach was followed by Andrews J in the first-instance decision in *ENRC*.\(^{102}\) On
appeal, the court held that whether *Three Rivers No. 5* was correctly decided regarding the
nature of a ‘client’ was a matter for determination by the Supreme Court.\(^{103}\) The court did
indicate, however, that there was ‘much force’ in the submissions that if *Three Rivers No. 5*
did lay down a restrictive interpretation of ‘client’, then it was wrongly decided.\(^{104}\) The court
said that ‘if, therefore, it had been open to us to depart from *Three Rivers (No. 5)*, we would

\(^{95}\) European Data Protection Board EU–US Privacy Shield – Third Annual Joint Review, adopted on

\(^{96}\) Paragraph 25, P7, European Data Protection Board EU–US Privacy Shield – Third Annual Joint Review,

\(^{97}\) *The Civil Aviation Authority v. Jet2.Com Ltd* [2020] EWCA Civ 35.

\(^{98}\) *Director of the SFO v. Eurasian Natural Resources Corporation Ltd* [2017] EWHC 1017 QB.

\(^{99}\) *Raiffeisen Bank International AG v. Asia Coal Energy Ventures Limited & Anor* [2020] EWCA Civ 1; *The

\(^{100}\) *Re The RBS Rights Issue Litigation* [2016] EWHC 3161.

\(^{101}\) ibid.

\(^{102}\) [2017] EWHC 1017 (QB).


\(^{104}\) ibid., Paragraph 124.
have been in favour of doing so’. 105 Hickinbottom LJ also had sympathy for this position in a recent Court of Appeal judgment and, while he felt ‘disinclined’ to follow Three Rivers No. 5, he stated that he was ultimately bound to do so. 106

V YEAR IN REVIEW

In January 2020, Transparency International released its annual Corruption Perception Index, in which the UK remained out of the top 10 for public sector transparency for the second year in a row. The Chief Executive of Transparency International UK commented that: ‘These results are a stark reminder that there is no room for complacency in the fight against global corruption. While the UK made some significant strides to tackle dirty money in recent years, it is deeply concerning to see its score relating to perceived public sector corruption stagnating. The new Government now has an opportunity to pull the UK back into the top 10. To do so it will need considerable ambition that will put anti-corruption front and centre of public policy both at home and abroad.’ 107

Boris Johnson’s election victory on 12 December 2019 brought to an end the uncertainty over the UK’s withdrawal agreement, more than three years after the referendum decision to leave the EU, in June 2016. The UK officially left the EU on 31 January 2020 and has now entered into a transition period that is expected to end on 31 December 2020. Since then, the global outbreak of covid-19 and the subsequent lockdown in the UK has left no opportunity to introduce and debate any new legislative initiatives to tackle corruption.

In contrast to the previous financial year, the SFO had a busier year in 2019/2020; albeit with mixed fortunes once again. Lisa Osofsky has had success with DPAs, with three settlements, including a record-breaking settlement with a major manufacturer of commercial jets. Together, the DPAs with Serco Geografix Limited, Güralp Systems Limited and the major manufacturer of commercial jets have seen receipt of nearly £25 million in financial penalties and costs; with over €400 million to be paid by the major manufacturer of commercial jets in fines and costs and a further €586 million in disgorgement, as part of its settlement. 108

The DPA between the SFO and Tesco plc also came to a successful conclusion in April 2020, with all of its obligations during the three years of its agreement completed, including the implementation of an ongoing compliance programme. This provided some evidence for the merits of a well-structured and considered DPA regime.

As previously referred to, the SFO issued its much-anticipated Corporate Co-operation Guidance, in August 2019, setting out, in substantial detail, the steps that the SFO expects corporations to undertake to be eligible for cooperation credit when the SFO makes charging decisions, including guidance relating to whether a DPA would be appropriate. 109 The SFO

---

105 ibid., Paragraph 130.
also updated its Operational Handbook for evaluating the effectiveness of compliance programmes in January 2020, providing further guidance to companies on what the SFO assesses during its investigations.\footnote{www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/}

By contrast, the acquittal of three Barclays executives in March 2020, following the dismissal of charges against the bank back in May 2018 and against John Varley, former CEO of Barclays, in April 2019, is a significant blow to the SFO. The dismissal of the charges against the bank has led to renewed calls for further governmental consideration of the law of corporate criminal liability.

The use of unexplained wealth orders has amassed further criticism over the last year. The Kazakh family recently won their challenge against the NCA in the High Court regarding three high-value London properties. Deciding against the NCA, the court held that the properties were legally owned and the NCA’s assumptions were ‘mistaken’ and ‘unreliable’.\footnote{National Crime Agency v. Baker & Ors [2020] EWHC 822 (Admin).} The defeat ‘highlighted major weaknesses in the UK’s defences against dirty money that should be addressed urgently’.\footnote{www.transparency.org.uk/press-releases/unexplained-wealth-order-uwo-dismissed-london-nursultan-nazarbayev-dariga-nazarba-nurali-aliyev/}

In May 2019, the government published its response to the House of Lords Select Committee’s post-legislative scrutiny report on the BA 2010. The response was on the whole non-committal, and largely noted the views of the House of Lords. However, in response to the Lords’ concern regarding the SFO’s slowness in bribery investigations, the government stated: ‘their current Director has emphasised that speeding up the pace of their investigations is a key priority for the organisation. Accordingly, the SFO’s Business Plan for 2019/20 outlines how SFO will speed up fraud and bribery investigations. The plan focuses on the delivery of four key priorities around: Operations, People, Stakeholders and Technology . . . Technology priorities include enhancing the use of Artificial Intelligence, predictive analysis and a new document and case management system to improve the management and review of the vast quantities of evidential material they collect’.\footnote{https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/800930/govt-response-hol-select-committee-bribery-act-2010.pdf.} No doubt the implementation of this Business Plan will be watched carefully over the coming year.

The Council of Ministers adopted the long-awaited EU Whistleblower Directive in September 2019. This rectifies what had been fragmented protection for whistle-blowers throughout the EU and guarantees a high level of protection for whistle-blowers who report breaches of EU law, including prohibition of all forms of retaliation and protecting confidential whistle-blowing. All 27 Member States will have until 2021 to comply and put the provisions into national law. However, at this stage the UK government has stated it will not implement the EU Whistleblower Directive but is committed to reviewing the UK’s whistle-blowing framework ‘once the recent reforms have built the necessary evidence of their impact. As part of this we will look at the protections offered in other countries’.\footnote{http://europeanmemoranda.cabinetoffice.gov.uk/files/2019/10/20191002_AppA_-_HoC_Letter.pdf.} Following the collapse of businesses such as Flybe and Patisserie Valerie, the FRC continues to come under criticism for its apparent weakness compared to other regulators and recent research has called for firmer action to hold companies and their auditors to account. The FRC strategy for 2020/21 calls for further progress to be made in the FRC’s transition to
the new regulatory body, the Audit, Reporting and Governance Authority, which will provide a new interventionist mandate to try to breach the delivery gap between what auditors say they will do and what they actually do, new leadership and stronger statutory powers. The Chief Executive of the FRC, Sir Jonathan Thompson, stated: ‘The strategy builds a bolder, more forceful regulator that will act with pace in supervising and holding companies to account’. Only time will tell whether the reality matches the rhetoric.

VI CONCLUSIONS AND OUTLOOK

Brexit was expected to remain at the forefront of political debate in the coming year, especially since the UK has now left the EU and entered into a transition period, following which EU laws and directives will no longer be legally enforceable in the UK. However, the global outbreak of covid-19 has instead dominated politics, leaving little political time or energy for new initiatives to tackle bribery, corruption and economic crime.

The covid-19 pandemic has also resulted in major delays in the English courts, with jury trials severely disrupted in a way that will likely have a lasting effect on the English courts’ timetable in the years to come.

The government has called for regulatory bodies such as the SFO and NCA to focus and do more to fight corruption and economic crime. Given the difficulties these bodies have faced over the last year, it remains to be seen whether they will be able to fulfil those expectations.

Chapter 11

FRANCE

Antoine Kirry, Frederick T Davis and Alexandre Bisch

I  INTRODUCTION

Criminal and administrative investigations in France – whether purely domestic or part of transborder activity involving other countries – follow procedures and principles that are fundamentally different from those in the United States. On a very general level, it is sometimes said that criminal justice in France is based on ‘inquisitorial’ principles whereas in the United States (and other common law countries) it is ‘accusatory’. The distinction is neither scientific nor complete, and as a practical matter the differences can be exaggerated. It is nonetheless true that many fundamentals differ from the US equivalents. These include:

a  the relative roles of prosecutors, judges and private attorneys;

b  the importance of state actors in establishing the facts of a case;

c  the relative absence of attributes of an ‘adversarial’ process, such as cross-examination;

d  the limited (but evolving) ability to negotiate with the investigating authority;

e  the nature and use of testimonial and other kinds of evidence; and

f  the absence of ‘rules of evidence’ comparable to those applicable in US courts.

As a result, anyone involved in an investigation of any sort in France must consult closely with local counsel.

i  Criminal investigations

Criminal investigations involve potential violations of the criminal laws, which are generally found in the French Criminal Code and the procedures for which are found in the French Code of Criminal Procedure (CPP).² Criminal violations are divided into three categories, which determine maximum sanctions, the courts involved and participants in the process. High crimes are criminal matters punishable by more than 10 years in prison. A person accused of a high crime has a right to a jury trial in a special court called the assize court. Ordinary crimes are violations punishable by imprisonment of between two months and 10 years and by financial penalties; the crime of corruption and most business crimes fall within this category. They are tried before the local district court, of which there is one in

---

¹ Antoine Kirry is a partner, Frederick T Davis is a retired partner and Alexandre Bisch is an international counsel at Debevoise & Plimpton LLP
² Both these codes are available in English at www.legifrance.gouv.fr/Traductions/en-English/ Legifrance-translations.
each significant city throughout France. There is no jury trial. Misdemeanours are violations punishable by financial penalties and may be tried in lower courts, of which there are several sorts in different locations.

Upon entry of the final judgment, an appeal may be taken to the relevant court of appeals. The proceedings in a court of appeals amount virtually to a new trial and the appellate judges – and, in the case of high crimes, the appellate jurors – can substitute their own finding of facts for those from the first trial and enter their own judgment of guilt or acquittal. Upon entry of a judgment in a court of appeals, an unsuccessful party may seek review from the Court of Cassation, the ‘supreme court’ for judicial matters, which can review the judgment only for issues of law and will either affirm the judgment or reverse it and remand to a new court of appeals.

Criminal investigations in France generally fall into two categories: regular and simple matters, which are handled by the public prosecutor; and complex and important matters, which are referred to an investigating magistrate.

Public prosecutor-led investigations represent more than 97 per cent of all criminal cases. In those cases, the public prosecutor works with the police – of which there are many national and local agencies, including specialised units – to investigate a matter and build an evidentiary record. In contrast to the judicial investigation discussed below, suspects have very little right to participate and defend themselves at this stage. When the public prosecutor is satisfied with the record, the matter is referred to the relevant court, which will generally be local to the place of infraction and may depend upon the severity of the accusation. At that time, the accused and his or her counsel will have access to the file, which will serve as the basis to prepare for trial.

Public prosecutors would only request the appointment of investigating magistrates for cases that appear so complex that developing the facts on their own would be expected to take too much time and absorb significant resources, or involve actions that prosecutors cannot take on their own, such as requesting the placement of suspects in pre-trial temporary detainment. In practice, most criminal investigations involving international matters are likely to be addressed by an investigating magistrate, although this landscape may be gradually evolving towards a greater role of public prosecutors, as the recent Airbus case (discussed below) suggests.

Investigating magistrates are found throughout France. In some instances, they are teamed together in a group; for example, such a group in Paris includes the principal investigating magistrates who look into financial and other major business crimes, including corruption, tax fraud and insider trading. The appointment of an investigating magistrate is mandatory for high crimes. With regard to regular crimes, he or she can be authorised to commence an investigation by an order from the public prosecutor. In some instances, however, third parties with an interest in the matter – often victims but occasionally non-governmental organisations given standing under the CPP – may file a complaint with an investigating magistrate and, if given the status of ‘civil party’, become formal parties to the investigation with access to the file (and, ultimately, are parties to the trial and any appeal). An investigating magistrate proceeds in rem (i.e., the scope of his or her investigation is limited to the facts and the persons listed in the public prosecutor’s order). He or she is obliged to determine whether a violation has occurred and, if so, who may be responsible for it. If the investigating magistrate determines that there is ‘significant and corroborated evidence’ of the criminal responsibility of an individual or a company, that person is summoned to appear before the investigating magistrate and in the absence of a strong demonstration of non-responsibility
(such as a misidentification) will be put ‘under formal investigation’. This status is the rough equivalent of being informed that one is a ‘target’ under US Department of Justice (DOJ) guidelines. Depending on the alleged offence, a person put under formal investigation can be placed under judicial supervision, including pretrial custody. A person against whom weaker evidence has been assembled, but who is still of interest to the investigating magistrate, may be designated a material witness, roughly the equivalent of being a ‘subject’ in the United States. Both a person put under formal investigation and a material witness have a right to formally appear in the investigative proceeding through counsel and to receive access to the entire file assembled by the investigating magistrate.

The investigating magistrate has a wide range of tools that may generally be exercised by the judge alone or with police. These tools include wiretaps, dawn raids on premises and custodial interrogations, in which a person may be held for questioning for 24 hours (subject to several renewal periods of 24 hours, depending on the violations, and up to a maximum of 144 hours for persons suspected of terrorism), usually in the presence of counsel.3 Interviews are generally reduced to a written statement, which the declarant is asked to sign.

When the investigating magistrate has finished an investigation, he or she will formally announce its closure and transfer the investigation file to the public prosecutor, who will then submit written opinion, copied to the parties to the investigation, as to which parties (if any) should be bound over to trial and on what charges. However, the position of the public prosecutor is not binding on the investigating magistrate, who can, and sometimes does, decide to bind parties over to trial even in opposition to the position of the public prosecutor, or vice versa. Because the public prosecutor’s views nonetheless have significant weight,4 the parties have an opportunity to file their own observations before a final decision is made by the investigating magistrate.

The investigating magistrate must issue a formal decision to close an investigation. There are two principal outcomes: either the person and the charges are dismissed, or the target is bound over to trial on specified charges. In unusual circumstances, an investigating magistrate can declare that he or she is without jurisdiction to proceed at all. The public prosecutor and a civil party may appeal a dismissal; however, parties bound over to trial cannot normally appeal such a decision. Throughout the period when they are formal parties to the investigation – whether under formal investigation or a material witness – the parties may be procedurally active through their counsel and can strategically intervene to influence the direction of the investigation. An example might be a formal request that the investigating magistrate search for certain evidence that might be exculpatory or appoint an expert on a certain matter. Such requests are often discussed informally with the investigating magistrate. Throughout the magistrate’s investigation, participants are bound by a secrecy obligation, making it a crime to disclose proceedings before the magistrate; this obligation, however, does not apply to the defendants, the victims and the press.

---


4 Neither prosecutors nor judges are considered lawyers in France, in the sense that they are not members of the Bar and they generally have not received professional training applicable to lawyers. Rather, both prosecutors and judges are considered as magistrates, and receive their professional training following law school graduation at the French National School for the Judiciary in Bordeaux. Prosecutors and judges thus tend to have somewhat closer professional relations with each other than either has with members of the Bar. Prosecutors nonetheless serve within the French Ministry of Justice and are not considered independent of the government.
Two differences from US investigative practices must be emphasised. First, before a person or a company is given the formal status of being under investigation or a material witness, there is little, if anything, that can be done to influence an investigation or prepare a defence, even if the party and its counsel are acutely aware that an investigation is under way (which is often the case if witnesses are summoned for interviews, or if there are dawn raids to obtain evidence). Before such a formal designation, any contact with an investigating magistrate would be viewed as irregular and improper, with negative consequences. Second, it is difficult for defence counsel to obtain information by interviewing witnesses or potential witnesses once any form of investigation has commenced, because any contact by a target or potential target (or counsel) with a percipient witness will almost inevitably be viewed as an attempt to influence that person’s testimony, with potentially dire results. As a result, members of French Bars tend to scrupulously avoid contacting witnesses in any disputed matter, including criminal investigations.

The investigating magistrate is required to conduct an impartial search for both incriminating and exculpatory evidence, and it is formally expected that the magistrate will establish ‘the truth’ of what happened. All the fruits of the investigation – including not only documents that are seized, but also witness statements based on custodial or other interviews – will be meticulously recorded in a file. At the end of an investigation, if the matter is bound over to trial, this file will be turned over to the trial court as part of the record before the trial judges and essentially will be the evidentiary basis for the trial. Because there are very few rules of evidence limiting proof that may be considered against the accused, including hearsay, in theory the evidence at a trial could consist of no more than the contents of the file assembled by the investigating magistrate, including the ‘testimony’ of witnesses only as set out in the formal record of their interrogations.

High crimes are tried before a jury consisting of three judges and six lay jurors chosen at random, all of whom deliberate together on both the culpability and the potential sentence. A verdict in a jury trial does not have to be unanimous. Guilt must be based upon at least six votes and sentence upon at least five votes (six if the maximum sentence is sought). Since May 2019, a new type of criminal court is being tested for a three-year period in seven local districts. This court has jurisdiction over high crimes punishable by up to 15 to 20 years in prison, except in case of recidivism. Trial will not take place before a jury, but before a panel of five judges.

The trial of a regular crime will be before either one or three judges. At trial, live witnesses may be heard if the presiding judge concludes that there is a meaningful dispute about that witness’s testimony and the defence may offer additional testimonial proof. The defendant (including a formally designated representative of a company) is expected to be at trial; while not put under oath, the defendant (or corporate representative) may be – and often is – questioned by the judges. No literal transcript of trial proceedings is kept, although the court clerk will keep notes (sometimes handwritten) of proceedings, which become part of the record. There is a presumption of innocence. Questions relating to the admissibility of evidence are rare and under the principle of ‘freedom of proof’, and judges may consider any evidence that they find useful. There is no hearsay rule as such, and formal written statements of witnesses are often in the record. The judges can convict only if they are convinced of guilt. The basis for a conviction or acquittal will be set out in a written judgment. There is no tradition of dissenting opinions.

A final judgment (including an acquittal) can be appealed to the court of appeals by a party dissatisfied with the outcome, and ‘cross appeals’ are often filed. The court of appeals
France

will then review the facts as well as the law de novo and reach its own conclusion as to both. Appeals from an assize or from a specialised criminal court decision of a high crime are to an appellate assize court, where the case will be heard by a jury of 12, consisting of three judges and nine lay jurors, with a majority of eight being necessary to convict (nine if the maximum sentence is sought). Appeals from a regular criminal court are to an appellate criminal court composed of three judges.

Victims claiming injury from a criminal act can, and usually do, pursue any damages claims in the same criminal proceeding, provided that they have applied for and been given the formal status of ‘civil parties’. In the event of a conviction, the criminal court will separately assess damages. Civil liability is generally linked to criminal responsibility. There are only limited circumstances in which a court can acquit a defendant of criminal responsibility but assess civil damages. Victims can also claim damages in a separate lawsuit before civil courts, but often choose to join a criminal matter to get the benefit of evidence assembled by the prosecution or the investigating magistrate. In some circumstances, the state may set up an administrative fund that compensates victims even in advance of a judicial proceeding, in which case the administrator of the fund may become subrogated to their rights to claim compensation from a defendant in a criminal trial.

Throughout an investigation and trial, including a custodial interrogation, a person under investigation has a right to remain silent. The right to silence is, however, invoked much less frequently than in the United States, in large part because of a common but strong inference in France – which is legally permitted – that a person otherwise in a position to do so who declines to explain his or her circumstances is acting out of an awareness of guilt. If a witness insists on a right to silence, there is no procedure to give that witness immunity as a predicate to forcing him or her to testify.

ii Administrative investigations

Scores of administrative agencies are empowered to conduct enquiries or investigations of one sort or another. Such matters are generally governed by specific laws, practices and procedures applicable to these agencies, including appellate review in some circumstances. The ultimate authorities for appeals against decisions from these administrative agencies are either the Court of Cassation or the Council of State, the latter functioning (in addition to other responsibilities) as a supreme court for administrative matters. In the international context, the two agencies most likely to be involved are the Financial Markets Authority (AMF) and the Competition Authority (AC).

Where market abuses are suspected, an investigation is carried out by the AMF, which can summon and take statements from witnesses, gain access to business premises and require any records of any sort. The AMF often works closely with the US Securities and Exchange Commission (SEC) and the DOJ, and frequently requests these authorities and other fellow regulators to gather evidence that may be of interest for its investigation. At the end of its investigation, if the AMF concludes that the evidence shows a market conduct violation, it must inform the criminal authorities so that a choice can be made between criminal or administrative prosecution. For many years, market abuses were prosecuted and sanctioned by both the AMF and the criminal justice system, but in a landmark decision of 18 March 2015, the French Constitutional Court reversed that long-standing position.

5 The French Constitutional Court (Conseil Constitutionnel) is the only body in France that reviews the constitutionality of French laws. In 2008, an amendment to the French Constitution introduced
France

A law passed on 21 June 2016 now ensures that suspects of market abuses are subject to one type of prosecution only, either administrative by the AMF or criminal by the public prosecutor or an investigating magistrate. Under both proceedings, a person found guilty of market abuse faces a maximum financial sanction of up to €100 million or 10 times any earned profit, or for legal entities, 15 per cent of annual consolidated turnover. Under criminal proceedings, a natural person also faces a maximum five-year prison sentence. If the authorities take the view that the alleged misconduct deserves a prison sentence, the tendency is to prosecute the case criminally. To date, however, most alleged market abuses are prosecuted by the AMF before its enforcement committee. Appeals are heard either by the Paris Court of Appeals and the Court of Cassation or the Council of State, depending on the status of the defendant. Prior to referring a defendant to its enforcement committee, the AMF may offer to enter into a settlement. Such a settlement does not amount to a conviction and the defendant is not required to admit the alleged facts, but must undertake to pay the Public Treasury a sum that cannot exceed the maximum pecuniary sanction applicable before the AMF enforcement committee.

Cartels are usually prosecuted and sanctioned as an administrative violation by the AC. The AC works very closely with competition authorities within the European Union and with antitrust authorities in the United States. The AC will generally align its rulings with those of European antitrust authorities. The maximum sanctions are €3 million for an individual and 10 per cent of the overall annual turnover, before taxes, for a legal entity enterprise. The calculation of an enterprise’s turnover for the purpose of applying the sanction is based on the highest turnover that was realised in any fiscal year following the fiscal year that preceded the one during which the practices were put into place. Final decisions by the AC may be subject to appeal before the Paris Court of Appeals.

II CONDUCT

i Self-reporting

The principles and practice of self-reporting are the subject of much debate in France and are evolving. The subject must be approached with great care.

In the area of competition law, self-reporting is encouraged. Since 2001, the AC has supervised a leniency programme that offers total immunity or a reduction of fines for companies involved in a cartel that self-report and cooperate by providing evidence. A settlement programme offers fine reduction for companies that elect not to challenge the objections filed by the AC. Under a commitment programme, AC investigations may also be stopped against companies that put in place or improve a competition law compliance programme.
In the area of criminal justice, a fundamental obstacle to self-reporting has been a general lack of statutory incentive to do so.\(^6\) Since December 2013, in the specific context of corruption and influence peddling, perpetrators or accomplices can have their prison sentence reduced by half if, by having informed the administrative or judicial authorities, they enabled the authorities to put a stop to the offence or to identify other perpetrators or accomplices. This incentive, however, does not apply to corporations. Recent efforts to expand the possibility of corporate guilty pleas have led to little change, although there are indications that that may be slowly changing. In December 2016, the legislature adopted the Sapin II Law,\(^7\) which established a procedure called a judicial agreement in the public interest (CJIP). A CJIP is quite similar to a US deferred prosecution agreement (DPA), which permits the disposal of claims of corruption, influence peddling, tax fraud and laundering of the proceeds of tax fraud without a criminal conviction. This procedure is available only to corporate entities. In June 2019, the French Financial National Prosecutor (PNF), together with the French Anti-corruption Agency (AFA), published its first guidelines on the use of the CJIP, providing that self-reporting within a reasonable timeframe will be taken favourably by the prosecution while considering whether to enter into a CJIP. The guidelines also state that self-reporting will be considered as a mitigating factor for the calculation of the fine. So far, in none of the 10 CJIPs approved to date does it appear that the company in question self-reported by bringing a matter to the attention of the French authorities before an investigation started. The absence of self-reports in those cases may be because they occurred in matters where the investigations – often led by investigating magistrates – had already commenced before the Sapin II Law was adopted.\(^8\) The PNF has emphasised that the great majority of his current investigations – more than 80 per cent during 2019 – are being handled as ‘preliminary investigations’; that is, without the involvement of an investigating magistrate. The Sapin II Law provides for a more flexible procedure for the negotiation of a CJIP during a preliminary investigation, and public prosecutors (including the PNF) clearly intend to use it aggressively.

**ii Internal investigations**

Internal investigations in the US sense must be approached very warily in France, for two reasons. First, there are a number of unusual local factors that may make the conduct of an internal investigation difficult; second, their actual function and ultimate use remain unclear and are evolving.\(^9\)

---

\(^6\) A further disincentive is the fact that, as noted in Section III.i, under French law a corporation may have a much greater ability than would be the case in the United States to claim that it is not responsible for the acts of employees or others apparently acting for it. This possibility makes it less attractive to engage in negotiations that implicitly give up the chance of a total acquittal under such a defence.

\(^7\) Law No. 2016-1691 of 9 December 2016.


\(^9\) For a general description of the challenges of conducting an internal investigation in a cross-border investigation involving France, see the article ‘Multi-Jurisdictional Criminal Investigations Pose Many Challenges’ published in the *New York Law Journal* on 18 November 2013 by the authors of this chapter.
Until recently, it was an open question whether a French lawyer could even participate in an internal investigation; many expressed the concern that a lawyer doing so might lose his or her independence or risk becoming a witness. These concerns were addressed by a thoughtful opinion of the Paris Bar issued in March 2016 and subsequent guidelines, which provide that lawyers can participate in internal investigations; they may do so even with respect to their usual clients; and the investigation would be covered by professional secrecy, the rough equivalent of (but in some respects markedly different from) the US attorney–client privilege. Particularly as the professional standards for conducting such an investigation develop, they should be handled carefully. The Paris Bar guidelines emphasise that an attorney conducting an investigation must be sensitive to the needs and vulnerabilities of the person being interviewed. This would certainly include the need to convey the equivalent of Upjohn warnings as practised in the United States – that is, to inform the person being interviewed that the interviewer is an attorney for the company, but that no professional privilege exists to the benefit of the person being interviewed – but would also imply a need to be especially careful about a witness who may give self-incriminating information and often to inform the witness of a right to consult with an independent attorney. Further, many aspects of EU and French law are protective of the rights of individual employees and other individuals and are generally hostile to sharing certain kinds of information, particularly outside the European Union or France.

Separate from the question of whether and how an internal investigation can be conducted is the question of how to use its fruits. A report that is solely used internally by the company and its lawyers to evaluate risk, devise strategy or adopt changes would raise no problem because it fits within the professional privilege. Much more problematic, however, is sharing the fruits of an investigation with a third party, particularly an adversary such as a prosecutor or investigative agency. Professional secrecy in France prohibits a lawyer who has conducted an investigation from sharing it with a third party, even with the consent of the client; in this respect, it is significantly different from the US attorney–client privilege. The client, however, is not under any professional restriction and can share a lawyer’s report with a third party or adversary.

Investigations that are carried out in contemplation of disclosure to non-French public authorities, and certainly those carried out in coordination with (or in response to a subpoena or a demand from) them, encounter more formidable obstacles. The Blocking Statute prohibits – and provides criminal sanctions for – transmittal of much documentary and testimonial evidence in France to officials in other countries. By its terms, the Blocking Statute would appear to apply primarily to a person or company making any direct response (that is, without going through international conventions on a state-to-state basis) to a foreign judicial or administrative discovery request, subpoena or the like. Although no court to date has so held, the leading view is that even private information gathering in France by a company or its attorneys with a view to sharing that information with investigative authorities in France.

---

other countries may violate the law. Further, if a company obtains data in France pursuant to a purely private investigation, removes that data from France and subsequently makes a decision to turn that information over to a foreign investigative authority, that company may be in violation of the Blocking Statute pursuant to the French principles of extraterritoriality (see Section IV.i).

If a company determines that data or other information that is in France should be shared with investigative authorities outside the country, the only formal means of doing so in strict compliance with the Blocking Statute is to proceed under the terms of an international convention, such as the US–France Mutual Legal Assistance Treaty (MLAT) or the 1970 Hague Evidence Convention. While a formal procedure under these instruments may sometimes take months, practical workarounds may be possible in certain areas. For example, the AMF and its foreign counterparts have increased their practical coordination through the Multilateral Memorandum of Understanding of the International Organisation of Securities Commissions. In the application of this Memorandum, the SEC is able to ask its sister agency in France to issue a request for information in France that the company is perfectly willing to produce but is barred by the Blocking Statute. The company thus produces the information in France to the AMF for immediate transfer to the SEC. One obvious consequence is that the AMF thereby becomes aware of the underlying investigation (if it has not already been so) and may, depending on the facts and the importance for French interests, commence its own. Interestingly, in the CJIP concluded with Airbus as part as the company's global resolution with the French, UK and US authorities, the PNF indicated that it shared investigations documents with the DOJ in accordance with the Blocking Statute, which in practice implied recourse to the US–France MLAT.

### iii Whistle-blowers

The Sapin II Law adopted in December 2016 significantly increased the protection afforded to whistle-blowers. A whistle-blower is now defined by the statute as:

> a natural person who discloses or reports, in a selfless and bona fide manner, a crime or offence, a serious and clear violation of an international convention duly ratified or approved by France, a unilateral decision of an international organisation made on the basis of such a convention, of law or regulation, or a serious threat or harm to the public interest of which he has been personally aware.

Entities that fall within the scope of the Sapin II Law must put in place an internal whistle-blowing programme for employees to report behaviours or situations contrary to the company’s code of conduct relating to corruption or influence peddling. In applying the

---

13 In 2007, a Franco-American attorney was convicted under the Blocking Statute and fined €10,000 for interviewing in France a potential witness in a pending litigation in the US. The DOJ appears to recognise the risk posed to companies, and their lawyers, who collect information in France for transmittal to the DOJ. In several recent deferred prosecution agreements that have been made public, the DOJ has recognised that the disclosure or reporting obligations of the company to whom the DPA applies, as well as any monitor acting under its authority, must comply with the French Blocking Statute. See, e.g., *US v. Alcatel-Lucent*, SA, 1:10-cr-20907-PAS (S.D. Fla. 2011); *US v. Total*, SA, 1:13 cr 239 (E.D. Va. filed 29 May 2013).
law of March 2017 on the corporate duty of care, entities may also have to put in place an internal whistle-blowing system to report serious human rights violations, serious bodily injury and environmental damage.

Whistle-blowers are protected against retaliation by an employer for providing accurate information of corporate wrongdoing to a competent authority. There is no provision in any French law for whistle-blowers to receive a reward or other payment from authorities. However, since 2017, the French tax administration may reward ‘informants’ who report misconducts relating to specific French provisions governing international taxation. The amount of the reward is calculated by reference to the evaded amounts. Informants are not considered as whistle-blowers and do not, as such, benefit from the protection of the Sapin II Law, although their identity and the reward are kept confidential.

III ENFORCEMENT
i Corporate liability

Article 121-2 of the French Criminal Code (CP) provides that a corporate entity can be held criminally responsible for the acts of its ‘organ or representative’ carried out for the benefit of the corporation. The statute specifies that this responsibility is not exclusive of individual responsibility for the persons involved.

Because of the relative recentness of this provision, which has existed in its current form since 1994, prosecutorial policies and practices, as well as details of the application of the law by the courts, remain surprisingly uncertain. The courts are still exploring, for example, the relative seniority or importance of an officer or employee necessary to qualify him or her as a representative of the company sufficient to trigger application of the statute. Separately, the courts are unclear whether a corporation can be held criminally liable without a specific finding as to which individual had committed acts deemed to be binding on the corporation.

In November 2012, a court of appeals acquitted Continental Airlines of criminal fault in the crash of a Concorde supersonic jet at Charles De Gaulle Airport, noting that the employee whose negligence may have caused debris to be left on the tarmac, and which contributed to the crash, did not have a sufficiently clear or established set of responsibilities upon which to justify corporate responsibility.15 In January 2015, another court of appeals entered into a judgment of acquittal of a large French company that had been convicted of overseas corruption for participating in the payment of an apparent bribe to obtain a large contract in Africa.16 Notably, the public prosecutor sought the corporation’s acquittal on the ground that the individuals who had been shown to have made certain payments were not shown to have had sufficient authority to bind the corporation. The court of appeals did not reach that issue because it acquitted the corporation (and its officers) for lack of sufficient evidence. In March 2018, in another case of overseas corruption, the Court of Cassation

---


15 Versailles Court of Appeals, 29 November 2012, No. 11/00332.

16 Paris Court of Appeals, 7 January 2015, No. 12/08695.
affirmed the conviction of the oil giant company Total SA on the ground that the offence had been committed on its behalf by its executive committee, which was composed of some other individual defendants.17

ii Penalties

Both corporate and individual criminal penalties, whether financial or imprisonment, tend to be significantly lower than in the United States, but things are changing.

The maximum penalties for any offence will be found in the statutes in articles generally adjacent to those specifying the elements of the offence. These provisions may provide for enhancement under individual circumstances, such as those involving recidivism or predation upon a minor or other vulnerable person. There are also general enhancement principles with respect to recidivists, to whom mandatory minima may apply. Generally speaking, courts do not multiply sanctions by treating separate victims of a crime – for example, serial victims of a single or continuing fraud – as separate counts, as is often the case in the United States.

Corporate penalties are also usually very low by US standards. The only two corporations convicted in France, by a final decision, for corruption of foreign officials were sentenced to fines of €300,000 and €750,000.18 The latter, however, amounted to the maximum fine faced by a corporation at the time of the offence. In December 2013, the maximum penalties applicable to criminal convictions for corruption were increased, and are now, for individuals, five years in prison and a fine of up to €1 million or double the profits gained from the offence, and for legal entities, a fine of up to €5 million or 10 times the profits gained from the offence. Legal entities convicted of ‘laundering’ now face a fine of up to 2.5 times the value of the goods or funds subject to the laundering operations; on that basis, in February 2019, the Paris criminal court fined UBS AG €3.7 billion for illegal solicitation of financial services and aggravated laundering of the proceeds of tax fraud.19

Individuals convicted in France of corporate crimes from which they did not personally benefit (but rather accrued benefits for their employer) are not generally given a prison sentence. Corporate fines are also moderated by the absence of the US penchant for cumulating ‘counts’ charging the defendant with separate violations when the overall conduct included repeated criminal acts (such as multiple payments in a bribery context).

With respect to both individuals and corporations, the sentencing provisions generally permit an array of complementary sanctions. These may include confiscation of the proceeds of the corruption and, for corporations, revocation of licences to commit certain activities, publication in national or other press of its conviction, and disbarment from eligibility to respond to public bids. In addition, European rules may prohibit convicted companies from participating in public bids in other EU Member States.

Corporate entities entering into a CJIP (see Section II.i) have to pay a fine proportionate to the benefit secured through the illicit activity, up to 30 per cent of the company’s average

17 Court of Cassation, 14 March 2018, No. 16-82.117.
18 ibid.

© 2020 Law Business Research Ltd
annual turnover for the previous three years. In January 2020, Airbus agreed to pay €2.1 billion to settle criminal charges with the PNF, which represents the highest fine imposed since the creation of the CJIP.20

iii Compliance programmes
The Sapin II Law adopted in December 2016 fundamentally changed French law with respect to compliance programmes. The law established the AFA, which among other things is tasked with supervising the new requirement, added by the same law, that all French companies, other than very small ones, adopt a compliance programme meeting certain specifications. The enforcement committee of the AFA is empowered to impose an administrative fine of up to €200,000 against individuals and up to €1 million against legal entities that do not comply with this law. The AFA appears to be vigilant about insisting on enforcement of this mandate.21 Since its creation, only two companies were referred to the enforcement committee, which eventually did not impose any fine.

French criminal law does not, at this point, include a ‘compliance defence’ that would permit a corporation to defend corruption or another charge by insisting that the individuals in question violated company rules or practices. However, a company that can show that employees committed acts in violation of company rules would certainly be better able to negotiate a CJIP or other outcome, and may even be able to claim an absence of criminal responsibility under Article 121-2 of the CP, as noted in Section III.i.

iv Prosecution of individuals
Individual officers and employees can be, and often are, prosecuted with the companies they serve. In such a circumstance, the attorneys for the corporations and the individuals may decide to cooperate during an investigative phase and in preparation for trial, and the content of meetings held pursuant to these joint efforts would be completely protected from subsequent discovery or divulgation by professional secret. In most circumstances, and in the absence of consensual arrangements such as a CJIP or pressure from foreign authorities, it would be highly unusual for a company to ‘cooperate’ with investigating authorities by agreeing to turn over information that may incriminate its officers or employees, at least where they were acting to benefit the corporation. In other circumstances, however, the corporation may conclude that it was a victim of its employees’ actions and thus has an interest in joining a prosecution. In one highly publicised case, for example, a rogue trader at one of the largest banks in France was accused of engaging in unauthorised market transactions that cost the bank billions of dollars in losses; the bank participated in the criminal prosecution of the trader by appearing as a civil party seeking damages from its employee. The criminal conviction of the trader included an obligation by the defendant to repay his former employer


for the losses he caused. On review, the Court of Cassation ruled that since the bank had been partially responsible for the losses, it could not collect reimbursement of all those losses from the employee.22

French law recognises a form of vicarious or derived responsibility for company heads for grossly negligent or criminal acts committed on their watch. The theory is to establish clear lines of responsibility for offences committed by corporations. Heads of companies may thus be found liable for offences caused by the company they direct in situations where they did not prevent the occurrence of an event through normal diligence or prudence; they can escape or limit such criminal responsibility by showing that they had formally delegated that responsibility to others in the company.

IV INTERNATIONAL

i Extraterritorial jurisdiction

French principles concerning the extraterritorial application of criminal laws are generally based upon principles of nationality and territoriality: by and large, its criminal laws apply to French nationals and to conduct that takes place on French soil.

The point of departure is Article 113-2 of the CP, which provides that French criminal law applies ‘to infractions committed on French territory’ and notably when at least ‘one of the elements of the offence has been committed there’. Subsequent provisions address situations where a person acting in France is viewed as having aided and abetted a principal violation committed overseas, as well as the applicability to acts committed on the high seas and other specific situations. Article 113-6 of the CP provides that French criminal law is applicable to any high crime committed by a French person outside France, and to any normal crime committed outside France if it would be criminally punishable in the country where the acts took place. French criminal law may also be applicable to certain crimes committed outside France if the victim is French. In the specific context of acts of overseas corruption, French law now also applies to acts committed abroad by someone exercising business, in whole or in part, in France (regardless of the nationality of that person and of the victim).

ii International cooperation

France is a signatory to a variety of international treaties committing it to coordinate its substantive laws in areas of common concern, such as the OECD Anti-Bribery Convention of 1997, and international treaties concerning cooperation in the investigation of crimes, such the Hague Evidence Convention of 1970 and several others. It is also a signatory to a number of European conventions that facilitate the execution of arrest warrants and other criminal procedures within Europe. French authorities coordinate closely with European cooperation agencies such as Europol and Eurojust, and with Interpol. ‘Red notices’ communicated by Interpol are diligently pursued in France.

France has signed a number of classic bilateral extradition treaties; its execution of these is diligent, albeit somewhat complicated because it may involve both the judicial and the administrative branches of the government, with their separate appeals processes. Extradition from France to countries within the European Union is simplified, and quicker, based upon the application of European conventions, and France cooperates closely with other European

22 Court of Cassation, 19 March 2014, No. 12-87.416.
authorities in execution of European Arrest Warrants. An office with responsibility for international criminal mutual aid is maintained within the French Ministry of Justice to facilitate formal and informal exchanges of information with prosecutors and investigators in other countries and at international criminal tribunals.

In recent years, France has signed a number of MLATs and memoranda of understanding between investigative agencies, such as between the AMF, the SEC and other financial market watchdogs. Importantly, the practical level of communication and cooperation between these agencies has visibly increased. As an example, US authorities now succeed in obtaining freeze orders concerning assets in France in a number of days rather than weeks, as was previously the case. The US Embassy in Paris maintains an Assistant United States Attorney on secondment from the DOJ, and approximately four agents of the Federal Bureau of Investigation, who work closely with their French counterparts in facilitating mutual aid; in addition, the French Ministry of Justice maintains a liaison magistrate in Washington, DC, to perform a similar coordination role with the US authorities.

Until early in 2018, a series of decisions by the Paris courts offered some hope that a person or company that was convicted, pleaded guilty, or even entered into a non-criminal outcome such as a DPA in the United States, could avoid prosecution in France under the theory of *ne bis in idem*, which is the rough equivalent of the protection against double jeopardy in the United States. In particular, several courts noted that both the United States and France signed the International Covenant on Political and Civil Rights (ICCPR), which contains a *ne bis in idem* provision. On 14 March 2018, however, the Court of Cassation annulled these decisions and held that the ICCPR only protects against multiple prosecutions by the same sovereign.23 There remain some situations, however, where an outcome outside France will bar subsequent prosecution. France’s statutory provisions relating to territoriality (see Section IV.i) provide that if a French prosecution is based only on ‘extraterritorial’ principles, such as the nationality of the defendant or the victim, then a definitive criminal outcome abroad bars prosecution in France. However, if the French prosecution is ‘territorial’ – meaning that any constituent act of the offence took place on French soil – then a French prosecutor is free to proceed, irrespective of any outcome elsewhere. Separately, a number of European treaties – in particular the Convention for the Implementation of the Schengen Agreement,24 the EU Charter of Fundamental Rights, and Protocol No. 7 to the European Convention on Human Rights – include a *ne bis in idem* provision that generally means, with some exceptions, that a prosecution in one country in Europe bars new prosecution in another.

### iii Local law considerations

Local law considerations in France may affect international investigations more significantly than in many other countries.

The Blocking Statute (see Section II.ii) was specifically designed to impede the ability of foreign governments (particularly the United States) in obtaining information, even

---


24 The Convention for the Implementation of the Schengen Agreement provision has been liberally interpreted by the European Court of Justice to protect against multiple prosecutions.
indirectly, in France; its origins lie in concerns about sovereignty and resistance to the extraterritorial reach of other countries’ laws. While it is relatively rarely enforced and is viewed by many French commentators as overly broad, it nonetheless reveals a measured commitment to the needs of other countries to investigate their crimes. EU and local laws relative to privacy and data collection further emphasise the sometimes unique problems of gathering evidence in France.25

V YEAR IN REVIEW

It has been commonly acknowledged for years that France lagged behind other industrialised nations in its pursuit of overseas corruption, and perhaps other areas of corporate criminality as well. In the area of overseas bribery, four iconic French companies paid over US$2 billion in fines and other payments to the DOJ and other US authorities for crimes that almost certainly could have been pursued in France.

The appointment in 2014 of a PNF with enhanced responsibility and visibility in the area of business crimes, and the adoption of Sapin II Law in December 2016, were clearly intended to redress this imbalance. In May 2018, Société Générale SA entered into both a CJIP with the PNF and a DPA with the US authorities to settle charges of alleged corruption of foreign public officials. The bank agreed to pay €250.15 million to the French authorities and US$292.8 million to the US authorities; this CJIP was a key milestone of enforcement of the Sapin II Law, as it constitutes the first coordinated resolution between French and US authorities in a foreign bribery case. In January 2020, Airbus reached the largest ever global bribery-related settlement of US$3.9 billion with French, UK and US. Charges included alleged bribery of foreign officials and violation of US arms export regulations. The company agreed to pay US$2.29 billion to the PNF, US$1.09 million to the SFO and US$527 million to the DOJ. This settlement is significant as it marks that France now intends to vigorously enforce its anti-bribery statutes, in an effort to make cases involving French companies of less interest to the DOJ than has been the case in recent years. Also, French authorities have indicated that they intend to take action so that the French Blocking Statute becomes more credible, and is ultimately enforced, by their foreign judicial authorities.

VI CONCLUSIONS AND OUTLOOK

Until recently, an international company potentially subject to French prosecution often considered that threat to be relatively insignificant compared to the risk of prosecution in the United States. The new laws and recent settlements in France may change that analysis.

---

Chapter 12

GREECE

Ilias G Anagnostopoulos and Jerina (Gerasimoula) Zapanti

I INTRODUCTION

Criminal Investigations of corporate conduct are always initiated by the Prosecutor’s Office. A criminal investigation may be initiated by the Prosecutor or it may follow an investigation of a Regulatory Authority (e.g., the Hellenic Capital Market Commission, the Auditors of National Transparency Authority, the Hellenic Competition Commission, etc.). The Regulatory Authorities perform audits and investigations within the scope of their powers to ensure compliance of corporations with the regulatory rules. Most Regulatory Authorities are entitled to investigate corporate conduct, but they are not entitled to prosecute criminal acts. The power to prosecute is only awarded to the Prosecutor. In practice, it is usual to have combined investigations (regulatory and criminal) where the Prosecutor ultimately receives all evidence and evaluates how to proceed further with the criminal investigation or prosecution.

Apart from the Prosecutor’s Office with the First Instance Courts (throughout the country), two separate prosecuting offices have been established, by special legislation, with the aim of combating acts of corruption and serious financial crime:

a the Prosecutor against Financial and Economic Crimes is responsible for investigating serious financial crimes (large-scale fraud, serious tax offences and related acts such as money laundering); and

b the Anti-Corruption Prosecutor is responsible for investigating acts of corruption related to public officials (domestic and foreign) and cases of special public interest.

Depending on the type of offence or the capacity of the individuals involved, it is possible that corporate conduct will be investigated by one of these special investigating bodies.

Both the Financial and Economic Crimes Prosecutor and the Anti-Corruption Prosecutor have extensive powers to gain access to privileged information, such as tax records and bank records, and all information that could be required in the course of their investigation. They may request assistance by other enforcement agencies or the police for the purposes of their investigations and they may use resources from other enforcement agencies or regulatory bodies.

---

1 Ilias G Anagnostopoulos is managing partner and Jerina (Gerasimoula) Zapanti is a partner at Anagnostopoulos.
Apart from the ease of access to information, both special prosecutors’ offices have the power to seize property and assets related to the acts under investigation even at the earliest stages of an investigation. Special judicial authorisation is always needed to obtain the content of confidential correspondence.

Certain enforcement agencies and regulatory bodies are entitled to obtain information and conduct separate investigations for the purposes of compliance and regulation within administrative or related proceedings. Depending on the proceedings, these regulatory bodies or enforcement agencies may also obtain tax records and bank account information and they are entitled, or obliged on some occasions, to share this information with the prosecuting authorities.

A company is obliged in principle to cooperate with the authorities, at least in terms of providing requested information and documentation and providing clarification regarding transactions, specific business conduct, etc. In the majority of cases, the authorities will send a written request to a company to forward certain information or documents. Failure to comply with such a request usually has no direct consequences (unless otherwise provided for by law) but may lead to an unfavourable report by the authorities or an on-site search and seizure to obtain the requested material. An on-site search and seizure (dawn raid) may be conducted even without prior notice to hand over documents and information if it is suspected by the prosecuting authorities that evidence may be endangered or that valuable information may be lost if immediate action is not taken.

In all cases, a company may object to handing over certain documents or material (e.g., privileged commercial information or correspondence) and refer to the Prosecutor to resolve the issue. In practice, when an on-site search is in progress, the company does not have the power to refuse to hand over any material but may raise objections about the nature of the material taken (e.g., privileged information) when signing the confiscation documents, in which case the material is sealed and taken by the agency pending resolution of the issue by the judicial authorities.

On some occasions (depending on the scope and nature of investigation), the company may be requested to submit its views in respect of the issues under investigation or to offer evidence in its defence (of any type: witnesses, bank records, correspondence, etc.) contesting the views of the investigating authority (usually included in a draft report).

Under Greek Law, there is no basic set of rules regarding cooperation of an entity within the context of a criminal investigation. There are special sets of rules for specific offences (e.g., competition offences, tax offences) under specific regulatory procedures but no general provisions for cooperation and leniency within the context of a criminal procedure.

II CONDUCT

i Self-reporting

There is no general rule or obligation for self-reporting. A series of legislative measures have been passed to enable enforcement agencies to detect misconduct with or without a company’s cooperation. It is in this respect that accounting officers are obliged to report any type of suspicious activity (related to tax evasion, money laundering, etc.) if there are indications of misconduct.

There are, however, special provisions in numerous laws and regulations that stipulate self-reporting of internal wrongdoing and cover most aspects of business activity. In some fields or industries, provisions for self-reporting are more stringent (e.g., banking and financial
services), while in others there is no explicit provision for self-reporting (most commercial activities in the private sector); however, rules for reporting criminal acts to the authorities may apply (as a general legal obligation) and this might, to some extent, lead to a kind of ‘self-reporting’.

There are specific industries or fields in which self-reporting is a prerequisite to benefiting from leniency measures or for immunity provisions to apply. These provisions apply in cases of violations of competition law, market manipulation, exposure of corrupt practices of public officials, organised crime and terrorism. In any of these instances, the authorities can choose to impose lesser penalties or grant complete immunity. These provisions may apply to corporate entities only, to individuals only, or to both. Considering that in the majority of cases involving serious corporate misconduct the authorities may impose administrative penalties and measures affecting the company’s ability to continue and develop its activities, as a rule participation in a leniency programme is considered the better option for a company and implicated individuals.

Where leniency or immunity measures are provided for (e.g., cartel offences, corrupt practices or money laundering), the extent to which they apply depends on the type of information provided to the authorities. As a rule, effective and complete exposure of illegal practices may lead to lesser penalties or immunity from criminal prosecution or administrative sanctions. Immunity is usually provided for when the reporting of illegal practices is of such significance that it contributes substantially to the exposure of illegal activity or perpetrators.

ii Internal investigations

A business may conduct its own internal investigation on any occasion. Whether the results should be shared with the authorities depends on the results and the nature of the case, as there is no general rule for self-reporting (with the exception of certain aspects of business activities usually related to regulatory rather than criminal provisions). There is no general obligation of sharing results or findings of an internal investigation with the authorities, although the authorities have been pushing for the findings and supporting documentation to be disclosed.

If there is evidence of serious wrongdoing, the company may be left with no choice but to refer all gathered information to the authorities. It is important to keep in mind on all occasions that any report to the authorities by the company, especially in relation to its employees or clients, should be done carefully to avoid any possibility of it being held liable for filing false accusations. It is not expected, of course, that a case presented to the authorities be proven beyond any doubt, but care should be taken to forward information that indicates with some certainty that serious misconduct has taken place.

When conducting an internal investigation, a company typically examines documents and interviews witnesses. It is also quite common to retrieve and evaluate records (e.g., electronic evidence, financial transactions and payment schemes) and whatever else may be useful for establishing the facts of a case. If there are serious signs of misconduct, the employee is usually notified in case he or she wishes to have counsel present and it is for the employee to decide upon the presence of counsel.

Attorney–client privilege may be asserted at any time. It is not always easy, however, to determine what falls under this protection. Apart from the obvious privileged information (e.g., correspondence between the attorney and client), there are other forms of communication (e.g., memos, drafts of letters or other documented material) that may contain privileged information. In such cases, the company should indicate to the authorities that this
is indeed privileged information. The company is not expected to waive its rights or privileges (especially the attorney–client privilege) as part of its cooperation with the authorities. The company may, however, choose to waive its rights in whole or in part with respect to such privileges if it becomes necessary for the purposes of its defence in regulatory or criminal procedures. For documents and material protected by special legislation (e.g., patents), the company is entitled to deny access, to give limited access or to request that the material be handled by the competent authorities in accordance with special legal provisions.

In investigations that come to the attention of authorities with certain powers awarded to them by law (e.g., the Prosecutor against corruption), withholding information may not be possible because of special legal provisions.

iii Whistle-blowers

Cases reported by employees to the company (internal control, compliance or other) and employees reporting directly to the authorities should be differentiated. When dealing with employees reporting suspicions of illegal activity to the company, the latter has a variety of options and usually handles the matter in accordance with its compliance procedures. In such cases, it is important for the company to acquire as much information as possible and endeavour to avoid exposing the source of information in so doing. This is also good practice when trying to establish that the employee’s reported suspicions are substantiated and not the result of other motives.

The company may decide to refer the matter within its own internal controls or make ad hoc internal enquiries to decide whether the employee’s report is substantiated; if it is, it must then decide whether what has been reported should be looked into further or referred to the authorities. During this process, the company may decide not to involve the reporting employee, especially if it can corroborate his or her information through other sources or documentation; this is usually the case when the reporting employee is not involved in the illegal activity. However, if the employee is involved, the company faces further challenges in deciding how to use the information provided because, on the one hand, it needs the information to assess the seriousness of the situation but, on the other hand, it has to evaluate the effects of the employee’s conduct to date.

If an employee reports his or her suspicions directly to the authorities (without giving prior notice to the company’s compliance department), the company’s options are limited and will necessarily be determined by the conduct of the authorities; nevertheless, the company should try to acquire all necessary information with respect to the employee’s involvement in the reported activity. Whether the reporting employee should or could remain with the company is something to be decided after reviewing all the available information and depends a great deal on the particulars of each case.

Whistle-blowers may be considered as witnesses in the public interest, which results in complete protection from criminal prosecution with respect to offences such as disclosure of privileged information or filing a false complaint relating to the information the whistle-blower provides to the authorities.

Although there is still no complete set of rules in place for whistle-blowers, numerous legal amendments have been made to protect whistle-blowers who may face false prosecutions, discriminations or unfair treatment because they disclosed serious corporate misconduct. These provisions are found in various laws and usually do not offer a comprehensive context of protection. Further steps are being taken to introduce a more robust set of rules, also in view of the new EU Directive EU2019/1937.
III ENFORCEMENT

i Corporate liability

A company ‘acts’ through individuals that have been vested with the appropriate power and authority. Typically, these individuals are either the managing director, the chief executive officer or the manager (depending on the company and its infrastructure). Some laws provide specifically for the persons who may be held responsible ex officio for a company’s actions (e.g., under tax law and regulations, and in environmental offences) or the conditions under which a company may be held liable for the actions of its employees (e.g., money laundering laws and regulations, and corruption practices).

An entity (a company) is not criminally liable under Greek Law, which provides that only an individual may be liable for a criminal act. However, constant harmonisation with international corporate standards, and the need to adjust internal legislation to align with European and international instruments, has led to provisions for liability of entities in the form of administrative measures and fines, etc.

Due to this differentiation, an entity may not be prosecuted and is also not eligible for leniency measures in criminal proceedings (except special situations provided for by special legislation). Prosecution and leniency measures are applicable to individuals. An entity may, however, face a number of sanctions as a result of its directors or employees’ criminal misconduct.

Joint representation by counsel is not prohibited, in principle, but it may be incompatible with other provisions in respect of regulations for a lawyer’s conduct or the handling of privileged information.

Corporate conduct may be punishable in certain cases. In most provisions (e.g., anti-corruption, anti-money laundering, anti-cartel legislation), company conduct is punishable when linked with positive gains or advantages in relation to this conduct. In other words, the company is liable as an entity – notwithstanding individual liability of employees – when there is some type of profit, gain or advantage to the company. The severity of punishment in these cases (in the form of administrative penalties or fines) usually depends on the type of profit or gain, as well as the annual turnover of the company.

ii Penalties

The types of sanctions that may be imposed against a business depend on the activity of the company, the industry it belongs to, its size, any prior misconduct, the type and seriousness of the act, etc. Sanctions against businesses are provided for in a variety of laws in respect of negligent or deliberate misconduct and may be roughly classified in the following categories:

a fines, which are of fixed amounts (for certain types of misconduct) or calculated in relation to the severity of the act and the size of the company;

b suspension of the company’s ability to participate in public tenders or to request public funding – repeated misconduct may lead to a permanent ban;

c suspension of the company’s activity for a period of time, depending on the severity of the act; and

d revocation of a company’s licence (usually for repeated offences).

Sanctions related to criminal proceedings are imposed by the Financial and Economic Crime Unit, SDOE (following the latest legislative amendments). Other sanctions related to independent regulatory proceedings may also be imposed by other competent authorities.
(depending on the company's purpose and industry), including the Revenue Service, the Hellenic Capital Market Commission (for companies in the capital market), the Hellenic Competition Commission and the National Organization for Medicines.

Sanctions can sometimes be imposed cumulatively (e.g., a fine and suspension of activity or a ban from public tenders or public funding). It is also not unusual to have more sanctions imposed as a result of provisions of more laws or regulations, especially in financial or economic offences (e.g., a tax offence may be related or combined with violations of anti-money laundering regulations).

iii Compliance programmes

The existence of a compliance programme is necessary in some industries, in the sense that there are minimum legal requirements in certain types of activities that form a compliance programme. These activities are mainly banking, finance and development through public funding. Apart from the fields or industries in which a compliance programme is a necessity (e.g., banks), most upper- or high-level businesses have developed compliance programmes to enable them to detect and handle misconduct within the company. Having a compliance programme in force is, in principle, helpful to a company to prove that it complies with the minimum requirements of internal control and is also interested in promoting good corporate practice and business ethics. Having a compliance programme in force enables a company to respond efficiently to requests by the authorities and to show that there is real interest in resolving issues.

iv Prosecution of individuals

The company's conduct in cases of individual liability very much depends on the type of misconduct (negligent or deliberate), the seriousness of the actions, the position of the individual, among other things. It is customary for a company to coordinate with the individual's counsel when his or her action occurred as a result of his or her position in the company (e.g., administrative proceedings or criminal proceedings against a managing director for an environmental offence). Termination of an employee's contract is something that the company has to decide after reviewing the whole case and the consequences for the entity. In cases where the employee has acted against the company's best interests and the actions are the reason the government seeks his or her liability, the company may have no option but to terminate the contract to protect its interests, privileged information, etc. In the end, it is a strategic decision for the company to make, unless, of course, the particulars of the case are such that there is no option other than to dismiss the employee. This is especially the case when an employee is involved in large-scale and serious violations of his or her duties, has deliberately acted against the company's interests, or engaged in fraudulent activity against the company itself, its clients or the general public.

IV INTERNATIONAL

i Extraterritorial jurisdiction

The Greek state, as a matter of practice, applies its laws to companies for conduct within the country or for acts that have effects within the country. It is in this respect that the Greek authorities seek to impose the law on companies either registered in Greece or active in the Greek economy (e.g., companies with registered offices in other countries that have agencies or subsidiaries in Greece).
Imposition of civil or administrative sanctions by the government is mostly done through agencies with jurisdiction over the company because it is located in Greece or has some type of registered presence in the country.

### ii International cooperation

Cooperation with other countries’ law enforcement or prosecutorial authorities has become common practice in large-scale investigations. Special law enforcement agencies such as the SDOE have entered into agreements with similar agencies from other countries, which has enabled a more efficient and fast exchange of information. Agreements between agencies usually follow framework agreements or treaties between countries. In the case of Greece, most aspects of international cooperation are treaty-based.

In recent years, there has been a studied increase in the cooperation of special prosecuting and investigating task forces with the corresponding authorities in other countries (especially in Germany and Switzerland) by adopting more flexible and quick procedures.

There are two sets of rules applicable to this prosecutorial cooperation. One applies to cooperation with EU Member States (in these cases all procedures and functions are simplified and faster). In all other cases, provisions for mutual assistance apply (for investigating acts or requests for information).

Extradition of a person to another jurisdiction is possible and not uncommon. In typical extradition proceedings, there is a minimum set of requirements that the Greek state examines to accept or reject such requests; rejection of extradition requests is not very common. Examination of the extradition requirements is carried out by a court. Any individual whose extradition is requested may object to his or her extradition and is represented by a lawyer. A decision in favour of extraditing the individual is appealable. As a general rule, Greek citizens are not extradited to other countries.

Extradition proceedings between EU Member States are quicker and more simplified because of the provisions of the European arrest warrant (EAW). The requested individual may still raise objections to his or her surrender to the requesting party, but the review is generally speedier and mainly relates to the typical requirements of an EAW issuance. A decision in favour of the surrender is appealable; Greek citizens may be surrendered to other EU countries following an EAW procedure, unless they are being prosecuted in Greece.

### iii Local law considerations

When multiple jurisdictions are implicated, an international instrument or treaty is applicable in the first instance. If the relevant jurisdictions are all EU countries, EU law is applied; this is very similar to Greek law on the basic elements of procedure. If a bilateral or international treaty is in force (in relation to other countries), the provisions of the treaty are primarily applied. Treaties usually have specific provisions on how to handle privileged information or private data, but in some cases Greece reserves the right to refuse to forward requested information if it is against Greek law, or may reserve the right to forward it subject to approval from the competent authority (e.g., dealing with the protection of private data).

In large-scale investigations involving several jurisdictions, all investigations are usually carried out locally in accordance with Greek law and regulations. Exceptions may apply in cases involving national security or relating to Greece’s diplomatic relations, in which case different rules may be applicable (as set out in international or bilateral treaties).
V YEAR IN REVIEW

Parallel investigations (from regulatory authorities and the prosecutor) are undergoing, targeting pharmaceutical companies and the National Health Organisation. The aim of these large-scale combined investigations is to identify possible misconduct in the process of pharmaceutical supplies and mismanagement of state funds in the process of drug registration in the national prescription platform or clinical studies.

Part of this investigation concerns an international drug manufacturer, under scrutiny for possible corruption. The case is being investigated in parallel with other jurisdictions and there has been much publicity regarding the conduct of the Anti-Corruption Prosecutor. This is partly owing to the fact that the case is based on statements of unidentified or protected whistle-blowers in Greece and possibly other jurisdictions, implicating political or state officials.

This investigation deals with complex cross-border issues (e.g., admissibility of evidence, rules of disclosure, deferred prosecution proceedings) and liability (criminal and civil) under Greek law.

VI CONCLUSIONS AND OUTLOOK

Latest amendments in the Greek Criminal Code and the Greek Code of Criminal Procedure have introduced a set of rules on plea bargaining. These are very recent additions that have not been tested yet and so there can be no feedback at this point. It is expected though, based on past experience with ad hoc legislation, that these provisions will have a positive effect in expediting criminal procedures where the defendant is willing to admit the facts of prosecution in exchange of lesser sentences.

As regards acts of corruption and related money laundering, there are provisions on leniency or non-prosecution in exchange for disclosing vital information to the authorities. This is also the case with organised crime and terrorism.

One thing that still needs to be considered is the inclusion of immunity-leniency provisions in respect to entities. Most leniency or immunity procedures focus on the individual and not the corporate entity, which does not have criminal liability under Greek law. This difference between individual liability and corporate liability (always in the form of administrative penalties and fines) directly affects an entity’s ‘willingness’ to proceed with self-reporting when detecting internal wrongdoing.

An entity may face severe sanctions if criminal acts (e.g., corruption or money laundering) committed by individuals result in monetary gain or benefits for the same. While the individuals may be eligible for lesser sentences or even immunity when cooperating with the authorities, if exposing certain criminal acts, the entity is not, in principle, eligible for a lenient treatment or immunity.

In addition, the entity may face consequences not only in respect to a criminal case but also in respect to regulatory, administrative or civil proceedings, which may be initiated by the authorities. In the current legal framework, in principle, an entity may not be able to settle all parallel procedures by means of a compliance programme or effective cooperation with the authorities.
Chapter 13

HONG KONG

Wynne Mok and Kevin Warburton

I INTRODUCTION

The key authorities with investigative power in Hong Kong are the Securities and Futures Commission (SFC), the Independent Commission Against Corruption (ICAC), the Competition Commission (HKCC), the Hong Kong Police Force (HKPF), The Stock Exchange of Hong Kong Limited (SEHK), the Hong Kong Monetary Authority (HKMA), the Inland Revenue Department, the Office of the Privacy Commissioner, the Customs and Excise Department and the Companies Registry. The Department of Justice (DOJ) is empowered to prosecute most criminal offences. The SFC may prosecute certain summary offences, including summary market misconduct offences. The DOJ is responsible for prosecuting indictable offences.

In addition to the HKPF, agencies including the SFC, the HKMA, the ICAC and the HKCC may exercise a special power of investigation, namely to carry out dawn raids, permitting entry to a company’s offices or an individual’s home without notice to investigate relevant potential misconduct. Authorities such as the SFC and the HKCC are also empowered to compel attendance at interviews. Moreover, unlike interviews before the HKPF or the ICAC where the person under investigation is protected by a constitutional right against self-incrimination, the SFC has the power to compel the interviewees to answer questions, where failure to answer or giving a false or misleading answer is a criminal offence. In addition, the SFC can compel the production of documents and records, including digital

1 Wynne Mok is a partner and Kevin Warburton is a counsel at Slaughter and May.
2 See Section 388 of the Securities and Futures Ordinance (Cap. 571) (SFO).
3 See Section 183(1)(c) of the SFO.
4 See Section 42 of the Competition Ordinance (Cap. 619).
5 A person facing a criminal charge shall be entitled to various minimum guarantees, including, among other things, not to be compelled to testify against himself or herself or to confess guilt. See Article 11(2)(g) of the Hong Kong Bill of Rights Ordinance (Cap. 383).
6 See Section 183(1)(c) of the SFO.
7 See Section 184(2) of the SFO; Note that pursuant to Section 187 of the SFO, such answers as an interviewee is compelled to give may not be used in subsequent criminal proceedings against the interviewee due to his or her constitutional right against self-incrimination.
8 See Section 183(1)(a) of the SFO.
devices (e.g. mobile phones and computers), information stored in or accessible through them and relevant access means (e.g. login names, passwords),\(^9\) and obtain a search warrant to search for and seize documents and records.\(^{10}\)

Domestic priorities often affect enforcement activity and the exercise of prosecutorial functions. For instance, anti-money laundering is a current enforcement priority for Hong Kong. In addition, various agencies publish their enforcement priorities each year and allocate their resources accordingly. For example, the SFC’s published enforcement priorities for 2019 included corporate fraud and IPO sponsor misconduct (both being top enforcement priorities), insider dealing, market manipulation, intermediary misconduct including mis-selling of financial products and money laundering.\(^{11}\) In October 2019, Ms Julia Leung, the SFC’s deputy chief executive officer, commented that the SFC was currently conducting a thematic review of the book building process in both equity and debt capital markets,\(^{12}\) indicating an emerging focus of the SFC’s enforcement action in 2020 and beyond. Under the ‘front-loaded’ approach introduced in 2017, the SFC focuses on the greatest risks facing the markets and intervenes at an earlier stage to address persistent problems and pre-empt the fallout from emerging threat.

Some regulatory agencies have published policies to encourage cooperation with their investigations. In April 2020, the HKCC published a revised ‘Leniency Policy for Undertakings Engaged In Cartel Conduct’ (the Leniency Policy for Undertakings)\(^{13}\) expanding upon the previous framework for leniency application established in November 2015. The HKCC also concurrently issued a ‘Leniency Policy for Individuals Involved in Cartel Conduct’ (the Leniency Policy for Individuals),\(^ {14}\) which for the first time allows an individual to report cartel conduct to the HKCC in exchange for leniency. Both policies were issued under the Competition Ordinance (Cap. 619) (Competition Ordinance), which provides that the HKCC may, in exchange for a person’s cooperation in an investigation or in proceedings, consider entry into a leniency agreement with the party under investigation, with the consequence that it will not bring or continue proceedings for a pecuniary penalty in respect of alleged cartel conduct. In April 2019, the HKCC issued the Cooperation and Settlement Policy for Undertakings Engaged in Cartel Conduct (the Cooperation Policy) for undertakings that do not benefit from leniency under the HKCC’s Leniency Policy for Undertakings. So far as other agencies are concerned, in August 2018, the HKMA issued its first ‘Guidance Note on Cooperation with the HKMA in Investigations and Enforcement

---

9 See Cheung Ka Ho Cyril and others v. Securities and Futures Commission [2020] HKCFI 270, a judgment made by the Court of First Instance of the Hong Kong High Court on 14 February 2020.
10 See Section 191 of the SFO.
Proceedings’ (HKMA Guidance on Cooperation), in which it stated that it would give recognition for cooperation and may offer reduction of proposed sanctions. In December 2017, the SFC issued its ‘Guidance Note on Cooperation’ (SFC Guidance on Cooperation), in which it stated that it would recognise and give credit for cooperation during an enforcement investigation when determining the applicable sanction.

II CONDUCT

i Self-reporting

Generally, a person (whether a company or an individual) is not obliged to self-report when it discovers internal wrongdoing; however, there are two key exceptions. First, a person is under a mandatory reporting obligation to the Joint Financial Intelligence Unit (JFIU) as soon as is reasonable or practicable if it knows or suspects that any property represents proceeds of an indictable offence or drug trafficking, or is terrorist property. Failure to make a notification to the JFIU when required to do so constitutes an offence punishable by a fine of HK$50,000 and up to three months’ imprisonment. Second, under the Code of Conduct for Persons Licensed by or Registered with the SFC, registered or licensed persons are required to immediately report to the SFC when there is any real or suspected breach or infringement of or non-compliance with any law, rules, regulations and codes administered or issued by the SFC. In addition, ‘failing to promptly and fully report a material breach’ may be regarded by the SFC as uncooperative conduct, which will be taken into account by the SFC when considering the appropriate outcome.

In the SFC Guidance on Cooperation, the SFC recognises voluntary and prompt self-reporting of any regulatory breaches or failings to it as a form of cooperation, which will provide the self-reporting person or organisation with the benefit of a reduction in sanction in disciplinary matters. However, in the case of an SFC-licensed corporation or registered institution, mere compliance with self-reporting obligations under the SFC rules will not amount to cooperation by itself. The SFC may enter into an agreement (Section 201 Agreement) to resolve disciplinary proceedings at an early stage pursuant to Section 201 of the Securities and Futures Ordinance (Cap. 571) (SFO) if it considers it appropriate to do so in the interests of the investing public or in the public interest. Cooperation from the regulated person and the extent and nature of such cooperation are factors considered by the SFC in exercising this discretion. As a general principle, the SFC is more willing to enter into a Section 201 Agreement if the regulated person demonstrates cooperation in the recognised

---

15 The JFIU is a joint reach force between the HKPF and the Customs and Excise Department.
16 See Section 25A of the Organized and Serious Crimes Ordinance (Cap. 455) and Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405), and Section 12 of the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575).
17 See Paragraphs 4.3 and 4.4 of the SFC Guidance on Cooperation.
18 See Paragraph 2.1 of the SFC Guidance on Cooperation.
19 Section 12 of the Securities and Futures (Client Securities) Rules, Section 11 of the Securities and Futures (Client Money) Rules and Section 11 of the Securities and Futures (Keeping of Records) Rules, Paragraph 12.5 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (SFC).
20 See Paragraph 3.1 of the SFC Guidance on Cooperation.
forms, or waives legal professional privilege, or commissions third-party reviews and gives directors’ undertakings to address the SFC’s regulatory concerns in accordance with the SFC Guidance on Cooperation.

Similarly, early and voluntary reporting of any suspected breach or misconduct is listed as an example of cooperation by the HKMA in the HKMA Guidance on Cooperation. However, the guidance note also provided that merely fulfilling statutory or regulatory obligations (e.g., self-reporting obligations and compliance with statutory investigation requirements) will not constitute cooperation.

The HKCC has also published the Leniency Policy for Undertakings and the Leniency Policy for Individuals to grant leniency to encourage self-reporting by companies and individuals that may have engaged in illegal activity, such as bid rigging or price fixing. Under these policies, leniency is available only for the first undertaking or individual involved in cartel conduct, who reports the cartel conduct to the HKCC and meets all the requirements for receiving leniency, provided that the undertaking or individual is not a ringleader of the cartel conduct. For individual applicants, leniency under the Leniency Policy for Individuals is only available before the granting of a marker to an undertaking under the Leniency Policy for Undertakings. In exchange for an undertaking’s or individual’s cooperation in the investigation of the cartel conduct, the HKCC will enter into a leniency agreement with the undertaking or individual and agree not to take any proceedings against them in any court in relation to the reported cartel, including proceedings for an order under Section 94 of the Competition Ordinance declaring that the undertaking or individual has contravened the First Conduct Rule. Under the previous leniency policy which allowed the HKCC to seek an order declaring contravention of the First Conduct Rule, there was a risk that the order may form the basis for follow-on damages claims by victims of the cartel conduct.

Undertakings that do not benefit from leniency under the Leniency Policy for Undertakings can opt to cooperate with the HKCC’s investigation under the framework of the Cooperation Policy in exchange for discount to the penalty issued.

ii Internal investigations

The authorities in Hong Kong are generally in favour of companies carrying out their own internal investigations provided they receive the results. The SFC Guidance on Cooperation specifically states that the forms of cooperation include making full and frank disclosure of information regarding breaches or failings and, in particular, providing information and

---

21 These forms include voluntarily and promptly reporting any breaches or failings to the SFC, providing true and complete information regarding breaches or failings, acceptance of liability and taking rectification measures. For more details, see paragraph 2.1 of the SFC Guidance on Cooperation.

22 See Paragraphs 6.2 and 6.3 of the SFC Guidance on Cooperation.

23 The First Conduct Rule prohibits an undertaking from (1) making or giving effect to an agreement, (2) engaging in a concerted practice or (3) as a member of an association of undertakings, making or giving effect to a decision of the association, if the object or effect of the agreement, concerted practice or decision is to prevent, restrict or distort competition in Hong Kong. See Section 6 of the Competition Ordinance (Cap. 619).

24 However, under the revised Leniency Policy for Undertakings, the HKCC may still issue an infringement notice to successful leniency applicants, who only report after the HKCC has opened an assessment or commenced an investigation, requiring them to admit a contravention, in order to permit the initiation of follow-on damages proceedings against them, if the victims have initiated follow-on action against other undertakings found to have contravened the First Conduct Rule.
evidence of which the SFC is otherwise unaware, including sharing the results of any internal investigation. In addition, the SFC now requires a licensed corporation (or a registered institution) to disclose information about certain internal investigations against a licensed representative or responsible officer (or in the case of a registered institution, an executive officer) who ceases to act in such capacity.\(^\text{25}\) In conducting an internal investigation, where there exists a concurrent investigation by the authorities, a company should be cautious and ensure it does not disclose the existence of the authorities’ investigations to a third party, including the employees, when conducting an internal investigation.

As in other jurisdictions, the typical means of carrying out an internal investigation include reviewing documents and interviewing relevant individuals. If interviews are conducted in the context of an internal investigation, it is not necessarily common for employees to retain their own lawyers, nor is there such a legal requirement in Hong Kong. Those present at internal interviews usually include in-house legal counsel, compliance or other specialised investigation team members. Depending on the nature and gravity of the potential misconduct, external counsel may also be engaged in the internal investigations.

Hong Kong law recognises legal professional privilege (including legal advice privilege and litigation privilege). Legal advice privilege applies to confidential communications between a lawyer and his or her client that comes into existence for the purpose of giving or obtaining legal advice. Litigation privilege applies to confidential communications between a party or his or her lawyer and third parties that come into existence for the sole or dominant purpose of preparing for actual or contemplated litigation. Thus, documents (e.g., minutes of meetings, interview notes) gathered or generated during an internal investigation for the purpose of giving or obtaining legal advice from a lawyer, or prepared for the dominant purpose of obtaining information or evidence for use in actual or reasonably contemplated litigation, can be privileged. However, one should bear in mind that privilege can be lost by giving or copying privileged documents to a third party, or referring to such documents for non-privileged reasons.

As for waiver of privilege, the SFC Guidance on Cooperation clarifies that a bona fide refusal to waive legal professional privilege attached to a document that would otherwise have to be provided to the SFC will not be regarded as uncooperative conduct, thus acknowledging legal professional privilege as a fundamental right protected by Article 35 of the Basic Law of Hong Kong and Section 380(4) of the SFO. Nonetheless, voluntary waiver of legal professional privilege over any document (including on a limited basis, i.e., the waiver of privilege is restricted to the specific party receiving the disclosed information) may be recognised by the SFC as amounting to cooperation, thus invoking the relevant leniency policy.

The HKMA has taken a similar stance. The HKMA Guidance on Cooperation suggests that the HKMA fully respects a person’s right to exercise legal professional privilege and the assertion of this right will not be regarded as uncooperative conduct. Nevertheless, voluntary

---

waiver of legal professional privilege in respect of one or more documents, even on a limited basis, may assist the HKMA’s investigation and will be taken into consideration when the HKMA assesses the degree of cooperation provided.

### iii Whistle-blowers

Although whistle-blower reports of potential illegal conduct are far from unknown in Hong Kong, the workplace culture may significantly affect the enthusiasm of some potential whistle-blowers actually to blow the whistle.

Employees may hesitate to come forward because of concerns about the effect on their own career prospects. Another reason for there being fewer examples of whistle-blowing than there might otherwise be may be the lack of incentive programmes in most of the regulatory regimes in Hong Kong (although the HKCC has published leniency policies for both undertakings and individuals to encourage whistle-blowing of cartel conduct).

As regards legal protection for whistle-blowers, although there are no stand-alone, comprehensive laws comparable to those in other common law jurisdictions, whistle-blowers can still obtain certain protections under statute or common law in Hong Kong.

First, there is the programme under the Witness Protection Ordinance (Cap. 564), which provides protection and assistance for witnesses whose personal safety or well-being may be at risk as a result of being a witness.26 If the Commissioner of the HKPF or the ICAC decides to include a witness in the protection programme or is assessing that person’s qualification for the programme, the relevant approving authority shall take such action as it considers necessary and reasonable to protect the witness’ safety and welfare.27

Second, whistle-blowers are protected from dismissal or discrimination under the Employment Ordinance (Cap. 57) if they are giving evidence in proceedings or inquiries relating to the enforcement of labour legislation, accidents or injuries to an employee or breach of the work safety regulations. An employer in violation of such protection by dismissing, threatening to dismiss or discriminating against a whistle-blower may be liable to pay a fine of HK$100,000 or compensate the whistle-blowing employee.

Third, whistle-blowers are protected from a claim of breach of confidentiality by various pieces of legislation and common law in respect of certain specified disclosures. Legislation offering this protection includes the Employment Ordinance (Cap. 57), Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405), the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) and the Organized and Serious Crimes Ordinance (Cap. 455). Common law also provides protection where it is in the public interest to make a disclosure relating to serious misconduct or important for safeguarding public welfare in matters of health and safety. In certain cases, whistle-blowing of possible corruption or bribery under the Prevention of Bribery Ordinance (Cap. 201) (Prevention of Bribery Ordinance) may constitute such a disclosure and is therefore protected under the common law regime.

A company receiving notification from a whistle-blower should be cautious in managing the information reported and the whistle-blower. Companies listed on the SEHK must follow the ‘comply or explain’ code provisions in the Corporate Governance Code in the Main Board Listing Rules to require its audit committee to review the arrangements its employees can use to raise concerns in confidence about possible improprieties in financial

---

26 See Section 3 of Witness Protection Ordinance (Cap. 564).
27 See Section 7 of Witness Protection Ordinance (Cap. 564).
reporting, internal control or other matters. The audit committee should also ensure that proper arrangements are in place for fair and independent investigation of such matters and for appropriate follow-up action.28

III ENFORCEMENT

i Corporate liability

When it comes to attributing criminal liability to a corporate entity for the conduct of its employees, whether corporate liability can be established depends on the type of conduct and the responsibility of the employee carrying out the alleged misconduct. If the potential liability arises from a statutory offence that imposes absolute liability on the employer (i.e., there is no need to prove fault on the part of the employer), then any such offences by an employee can result in the employer being held vicariously liable. Otherwise, only offences by senior employees (e.g., directors, senior managers, superior officers), who at the material time were the ‘directing mind and will’ of the company, can be said to be offences of the company. In such circumstances, a corporate entity may be held liable unless the offence is only punishable by imprisonment or can only be committed by natural persons in their personal capacity. However, as the burden of proof for criminal offences is high (beyond reasonable doubt), there are likely to be practical difficulties in establishing corporate criminal liability. In contrast, a plaintiff need only prove its case on a balance of probability to establish civil liability, a lower burden of proof. In addition, civil actions can offer more flexibility by potentially offering preventative and punitive remedies as well as damages.

As long as there is no conflict of interest arising between an employer and its employees, they can be represented by the same counsel. However, if the employee’s anticipated defence may contradict that of the employer, for instance, or the evidence to be given by the employee is against the employer, there may arise a potential or real conflict. In such circumstances, the parties should be represented by separate legal advisers.

ii Penalties

The enforcement actions that the SFC may take include disciplinary proceedings, civil proceedings before the Hong Kong High Court, criminal proceedings before the magistrates’ courts in Hong Kong, and proceedings before the Market Misconduct Tribunal (MMT).

For criminal market misconduct offences under the SFO,29 a person may face upon conviction on indictment a fine of up to HK$10 million and imprisonment for 10 years, or on summary conviction a fine of up to HK$1 million and imprisonment for three years.30

---

28 See Paragraph C.3.7 of Appendix 14 (Corporate Governance Code and Corporate Governance Report) of the Main Board Listing Rules.

29 Market misconduct includes insider dealing, false trading, price rigging, disclosure of information about prohibited transactions, disclosure of false or misleading information inducing transactions and stock market manipulation.

30 See Section 303 of the SFO.
The SFO also prescribes penalties for offences other than market misconduct. For example, a person who breaches Section 114 of the SFO by carrying on regulated activity without a licence is subject to a fine of up to HK$5 million and imprisonment for seven years.

The SFC may also seek civil remedies in either the MMT or the High Court for alleged market misconduct and other breaches of the SFO. These remedies include orders from the MMT, compensation by way of damages and injunctive relief granted by the Court of First Instance of the Hong Kong High Court. Orders available to the MMT include disqualification orders, cold shoulder orders, cease and desist orders, disgorgement orders, government costs orders, SFC costs orders, Financial Reporting Council costs orders and disciplinary referral orders. The injunctive relief the court may grant includes an order restraining or prohibiting a person from dealing in any specified property, an order appointing a person to administer the property of another person and other ancillary orders.

Under Part IX of the SFO, meanwhile, the SFC is empowered to discipline regulated persons for alleged misconduct or who may no longer be fit and proper to be licensed or registered. The range of sanctions that could be imposed include:

- a revocation or partial revocation of the licence or registration; suspension or partial suspension of the licence or registration; revocation of approval to be a responsible officer;
- suspension of approval to be a responsible officer; and
- a fine (up to HK$10 million or three times the profit gained or loss avoided, whichever is the higher); or private or public reprimand.

The range of potential sanctions will vary therefore depending upon the nature of the proceeding. Taking market misconduct as an example, the sanctions will vary depending on whether it is a civil or a criminal proceeding and, if criminal, whether it is on conviction on indictment (prosecuted by the DOJ) or on summary conviction (prosecuted by the SFC). As the civil and criminal regimes under the SFO are mutually exclusive, the SFC can choose only

31 Including failure to disclose interest in securities in accordance with Part XV of the SFO, carrying on a business in a regulated activity without a licence, and issuing unauthorised advertisements, invitations or documents to participate in a collective investment scheme.
32 An order prohibiting a person from being involved in the management of specified corporations. See Section 257(1)(a) of the SFO.
33 An order prohibiting a person from directly or indirectly trading in Hong Kong financial products which the SFC regulates. See Section 257(1)(b) of the SFO.
34 An order prohibiting a person from engaging in any specified form of market misconduct again. See Section 257(1)(c) of the SFO.
35 An order requiring a person to pay the government an amount equal to the profit made or loss avoided as a result of the misconduct. See Section 257(1)(d) of the SFO.
36 An order requiring a person to pay to the government costs of the inquiry, costs incidental to the inquiry and any costs of investigation for the purposes of the inquiry. See Section 257(1)(e) of the SFO.
37 An order requiring a person to pay to the SFC reasonable expenses in relation or incidental to any investigation of their conduct or affairs. See Section 257(1)(f) of the SFO.
38 An order requiring a person to pay to the Financial Reporting Council reasonable expenses in relation or incidental to any investigation of their conduct or affairs. See Section 257(1)(fa) of the SFO.
39 An order giving a copy of the report of the MMT proceedings to any regulatory body that may take disciplinary action against the relevant person. See Section 257(1)(g) of the SFO.
40 See Section 213(2)(c) of the SFO.
41 See Section 213(2)(d) of the SFO.
one regime under which to bring an action. Usually the SFC will refer all market misconduct cases to the DOJ for advice on the suitability of instituting prosecution. The SFC also must obtain consent from the Secretary for Justice before commencing an MMT proceeding.

iii Compliance programmes

It is important for companies to establish and maintain effectively functioning internal control mechanisms. Although having a compliance programme itself will not exempt a company from liability, it may be recognised as a mitigating factor in the application of sanctions. It may also reduce the risk of corporate liability arising from a breach by an employee, if it could be established that the employee’s misconduct was a result of breach of the internal policies established by the employer.

For implementing and improving anti-corruption compliance programmes, the ICAC has published various guidelines for different types of entities, such as listed companies, the catering industry, schools, etc. In its anti-corruption guide for listed companies, the ICAC recommends certain components to be covered by a company in its anti-corruption programme: an anti-corruption policy, guidance on ethical standards and anti-corruption for all company personnel, a mechanism for identification and assessment of corruption risk, anti-corruption control, and training and communication. However, these guidelines are more advice than ‘best practice’, as the Prevention of Bribery Ordinance does not regard compliance programmes as constituting a mitigating factor or allow them to be treated as a means to mitigate corporate criminal liability.

Notably, in the SFC Guidance on Cooperation, instituting necessary enhancements to internal controls and procedures is recognised as a potential rectification measure and form of cooperation. Thus, enhancing a compliance programme may, depending on the stage when cooperation is effected, allow the company to enjoy a reduction of sanction of between 10 and 30 per cent.

iv Prosecution of individuals

If an individual is to be prosecuted by government authorities, his or her employer should be careful in managing its relationships with stakeholders. The company may coordinate with the individual’s independent counsel, but should also bear in mind the risk of a conflict of interest arising, as the individual’s conduct may have compromised the company’s position not only in relation to the substantive offence but also reputationally.

The SFC Guidance on Cooperation does not expressly require a company to dismiss or take disciplinary action against an employee under investigation in order to show cooperation. Conversely, an employee’s compliance with a notice to attend an interview, for example, will not be regarded as cooperation that can lead to a leniency benefit. Indeed, were an employer to dismiss an employee because of his or her refusal to be interviewed by the company or the regulators, it may risk that dismissal being regarded as a wrongful dismissal and the company may be liable to pay damages. Thus, during the investigation stage, an employer may prefer, at least initially, to exercise its statutory entitlement to suspend an employee for up to 14 days pending the employer’s decision as to whether or not to terminate the contract.


43 See Paragraph 3.1 of the SFC Guidance on Cooperation.
of employment under section 9 of the Employment Ordinance.\textsuperscript{44} If the employee is found liable upon conclusion of the investigation, the company can then take disciplinary measures against that employee.

The company may pay the legal fees for employees under investigation. There is no adverse inference from such an arrangement, as long as the company is not enticing the employee to fabricate evidence.

\textbf{v} Sponsor misconduct

In March and May 2019, the SFC imposed record-breaking fines totalling HK$813.7 million against several international banks for their inadequate due diligence while acting as sponsors in a number of past Hong Kong initial public offerings. Some of the banks were reprimanded and the licence of one of the banks was suspended. As commented by Mr Ashley Alder, the SFC’s chief executive officer:

\begin{quote}
the outcome of these enforcement actions for sponsor failures – particularly failings when conducting IPO due diligence – signify the crucial importance that the SFC places on the high standards of sponsors’ conduct to protect the investing public and maintain the integrity and reputation of Hong Kong’s financial markets. The sanctions send a strong and clear message to the market that [the SFC] will not hesitate to hold errant sponsors accountable for their misconduct.\textsuperscript{45}
\end{quote}

In October 2019, Ms Julia Leung, the SFC’s deputy chief executive officer, reiterated the message that in respect of sponsor supervision the SFC have little tolerance for misconduct and will be resolute in upholding conduct standards,\textsuperscript{46} after highlighting five major failings in sponsor due diligence work as identified in a previous thematic inspection report.\textsuperscript{47}

\textbf{IV} \hspace{0.5em} INTERNATIONAL

\textbf{i} Extraterritorial jurisdiction

For criminal offences, the courts will be hesitant to claim jurisdiction over conduct occurring outside Hong Kong. However, the SFO extends liability for certain market misconduct taking place outside Hong Kong that affects the Hong Kong markets. This includes false trading, price rigging, disclosure of false or misleading information inducing transactions and stock market manipulation.\textsuperscript{48}

\begin{footnotesize}
\begin{enumerate}
\item See Sections 9 and 11(1)(b) of the Employment Ordinance (Cap. 57). Section 9 allows an employer to terminate an employment contract without notice or payment in lieu, if an employee: (1) wilfully disobeys a lawful and reasonable order; (2) misconducts himself or herself, such conduct being inconsistent with the due and faithful discharge of his duties; (3) is guilty of fraud or dishonesty; and (4) is habitually neglectful in his or her duties.
\item See footnote 12.
\item Namely: (1) adopting a box-ticking approach; (2) ignoring red flags; (3) deficient interview practices; (4) over-reliance on experts and third parties; and (5) improper supervision and inadequate resources.
\item See Sections 295, 296, 298 and 299 of the SFO for criminal offences and Sections 274, 275, 276 (disclosure of information about prohibited transactions), 277 and 278 of the SFO for civil equivalents.
\end{enumerate}
\end{footnotesize}
The Competition Ordinance has extraterritorial reach over agreements and conduct conducted outside Hong Kong but that have the object or effect of preventing, restricting or distorting competition in Hong Kong. 49

ii International cooperation

With regulatory misconduct becoming increasingly complex and cross-border, regulatory agencies such as the SFC, the ICAC, the HKCC and the HKMA actively seek to enhance cooperation with their overseas counterparts.

This is particularly common with regard to the SFC’s regime owing to the globalisation of securities and derivatives markets. In general, the SFC is empowered by Section 186 of the SFO to provide investigatory assistance to regulators outside Hong Kong if the SFC is satisfied that it is desirable or expedient to provide assistance in the interests of the investing public or in the public interest, or the assistance will enable or assist the overseas regulators to perform their functions and the assistance is not contrary to the interests of the investing public or to the public interest.

The SFC is one of the 124 signatories 50 to the International Organization of Securities Commission Multilateral Memorandum of Understanding (IOSCO MMOU) concerning consultation, cooperation and exchange of information. It also has bilateral collaborative arrangements for investigatory assistance or exchange of information with various overseas jurisdictions. 51

More notably, the SFC maintains a close partnership with the China Securities Regulatory Commission (CSRC) through the IOSCO MMOU, the Memorandum of Regulatory Cooperation, the enforcement memorandum of understanding (MOU) for the Mainland-Hong Kong Stock Connect, the MOU concerning futures, dated December 2017, the MOU concerning cooperation and exchange of information, dated December 2018 and the MOU concerning the obtaining of audit working papers in the Mainland arising from the audits of Hong Kong-listed Mainland companies, dated July 2019. 52

The international regulatory cooperation can also be illustrated by the framework for extradition and mutual legal assistance. Under the Fugitives Offenders Ordinance (Cap. 503), the DOJ is empowered to handle requests for the surrender of fugitive offenders. As regards providing mutual legal assistance, Hong Kong has mutual legal assistance agreements with 30 jurisdictions in force under the Mutual Legal Assistance in Criminal Matters Ordinance (Cap. 525) 53 for mutual assistance in criminal matters, including assistance in relation to giving evidence, search and seizure, production of material, transfer of persons to give assistance, and confiscation of proceeds of crime.

49 See Section 8 of the Competition Ordinance (Cap. 619).
50 Up to 26 September 2019, see www.sfc.hk/web/EN/about-the-sfc/collaboration/overseas/iosco-mmou.html, last accessed on 3 May 2020.
iii Local law considerations

When several jurisdictions are implicated in an investigation, the first Hong Kong statutory obligations one may have to bear in mind are secrecy obligations, for example those imposed by the SFO or the Prevention of Bribery Ordinance. Advance approval is needed from the SFC for disclosing relevant non-public information to foreign regulators. In addition, although personal data disclosure with consent is generally allowed under Hong Kong data privacy law, an employer is reminded to review the scope of the general consent (if it exists) given by employees, which may need to be supplemented by consent specific to the relevant investigation.

V YEAR IN REVIEW

2019 marks the 30th anniversary of the SFC and has seen some of its highest-profile activities to date, despite the unprecedented political and social challenges Hong Kong has been faced with since the second half of 2019. As stated by Julia Leung, the SFC’s deputy chief executive officer, in October 2019: ‘[t]he SFC imposed fines of over $900 million in disciplinary actions against eight sponsor firms and three sponsor principals over the past 30 months’. While this emphasises that the SFC’s focus is currently on the work of sponsors in initial public offerings, an emerging focus for 2020 and beyond is the book building processes in both equity and debt capital markets, in respect of which the SFC is doing a thematic review. In the reporting year 2018 to 2019, the SFC disciplined 21 corporations, four responsible officers and 10 licensed representatives, resulting in total fines of HK$940 million, almost twice the amount of the last reporting year. At the same time, only 238 investigations were started in the reporting year 2018 to 2019, down from 280 in 2017 to 2018 and 414 in 2016 to 2017. This echoes with chief executive officer of the SFC Ashley Alder’s suggestion that the SFC’s current tactics involve prioritising certain investigations so that the SFC could focus its finite resources on the most important cases. The SFC appears to be prioritising and focusing on the high-profile and serious matters, such that it is focusing on quality over quantity; while the number of investigations is getting lower, the aggregate level of fines imposed is getting higher.

Another trend is the SFC’s ongoing attempts to strengthen its relationship with its counterpart in Mainland China, as well as other local regulators. With respect to mainland China, the SFC has signed various MOUs with regulators like the CSRC, including one concerning the obtaining of audit working papers in the Mainland arising from the audits of Hong Kong-listed Mainland companies, entered into by the SFC, the CSRC and the Ministry of Finance of the People’s Republic of China in July 2019. Locally, the SFC entered into an MOU with the ICAC in August 2019 to formalise and strengthen cooperation

54 See Section 378 of the SFO.
55 See Section 30 of the Prevention of Bribery Ordinance (Cap. 201).
56 See footnote 12.
between the two authorities in respect of mutual provision of investigative assistance and capacity building.\(^5\) In April 2020, the SFC entered into an MOU with the HKCC to enhance cooperation and exchange of information between the two regulators.\(^6\)

Another new development by the SFC is in relation to virtual assets. The SFC introduced a new regulatory framework for virtual asset trading platforms in November 2019, which addresses key regulatory concerns in such areas as the safe custody of assets, know-your-client requirements, anti-money laundering and market manipulation, etc.\(^6\)

In terms of the HKCC’s enforcement actions, the HKCC continued the momentum in its fight against cartel conduct. Since 2019, the HKCC has brought three enforcement actions in respect of alleged cartel conduct such as price fixing, market sharing and bid-rigging. Notably, in addition to penalties against companies, the HKCC sought for pecuniary penalties and director disqualification orders against individual directors allegedly involved in the cartel conduct in its most recent four enforcement actions. This echoes with the message from the HKCC that not only companies, but also individuals who engaged in anti-competitive conduct may expect to face consequences for their actions.\(^6\) In 2019, the HKCC also welcomed two favourable judgments from the Competition Tribunal in the HKCC’s first two enforcement actions brought in 2017, finding multiple companies liable for bid-rigging (in the first case), and price-fixing and market sharing (in the second).\(^6\) In April 2020, the Competition Tribunal further rendered a judgment on pecuniary penalties against the companies found liable for price-fixing and market sharing in the second case.\(^6\)

On the policy front, the HKCC published a new Leniency Policy for Individuals and an updated Leniency Policy for Undertakings in April 2020, in order to further encourage cooperation with its cartel enforcement.

As for the HKMA, its work in 2019 was mainly on the areas of banking stability, smart banking, implementation of international standards, FATF/APG Mutual Evaluation,

---


consumer and investor protection, green and sustainable banking and capacity building. For 2020, credit risk management, supervision of virtual banks, operational and technology risk management, investor and consumer protection in digital age are among its top priorities.65

VI CONCLUSIONS AND OUTLOOK

According to the SFC’s annual report for 2018 to 2019, the SFC’s current enforcement priorities are in relation to corporate fraud, IPO sponsor misconduct, insider dealing, market manipulation and intermediary misconduct including mis-selling of financial products and money laundering. In respect of tackling misconduct by listed companies, according to a recent SFC Regulatory Bulletin, the SFC seeks to address regulatory concerns such as concealed share ownership and control, suspect valuations, warehousing of shares and nominee arrangements and highly dilutive rights issues.67

In response to the increasing complexity of insider dealing and market manipulation cases, the SFC will adopt the ‘One SFC’ investigatory approach, which emphasises cross-divisional collaboration. Focusing on failings that pose systemic risks, the SFC will deal with breaches by an intermediary together, in the same group, to increase deterrence. Under the new front-loaded regulatory approach, the SFC will also engage in targeted intervention at an early stage to suppress illegal, dishonourable and improper market practices.

Regarding a sponsor’s misconduct, the SFC concluded a number of high-profile sponsor misconduct cases in 2019, meting out penalties which include record-breaking fines totalling HK$813.7 million on five prominent banks for their inadequate due diligence work as sponsors in past IPOs, alerting sponsors to maintain the highest standards and to perform due diligence with professional scepticism. The record-breaking fines also reflect the increasingly tough stance taken by the SFC, which will likely remain the case in 2020.

As regards anti-money laundering, the SFC reprimanded and fined a brokerage HK$15.2 million in February 2019 for failures in complying with anti-money laundering and counter-terrorist financing regulatory requirements when handling third-party fund deposits.68 This represents the largest fine ever imposed under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615). Two months later in April 2019, the SFC further prohibited a member of the brokerage’s senior management who was also a responsible officer from re-entering the industry for 10 months.69

66 See footnote 11.

© 2020 Law Business Research Ltd
It is very likely that 2020 will see a continuing trend of strengthening enforcement actions against firms with internal control failures related to know-your-client or anti-money laundering requirements.

In respect of cross-border cooperation, with a growing number of SFC-CSRC MOU in place and Hong Kong’s listing regime continuing to attract high-profile listings by mainland China-based companies, there is little doubt that the aforementioned cooperation will remain strong (if not grow stronger) in 2020, given the closer connection between mainland China and Hong Kong, at both the regulator level and the market level.

Companies under SFC investigation would be wise to consider the consequences of the potential exchange of information and other investigatory assistance between the SFC and the CSRC, including the assistance the SFC may receive in obtaining audit working papers stored in mainland China under an MOU signed in July 2019.

Another observation is that opportunities and challenges coexist in new economies. On the one hand, the new listing regimes in Hong Kong, as reformed in 2018, support new economy companies and pre-revenue biotech firms. On the other, the SFC stepped up its regulatory oversight over virtual asset trading platforms in November 2019 by introducing a licensing regime that brings certain platforms within its supervisory remit. While the new regime is still at a nascent stage, the SFC already made it clear that a breach of a licensing condition would be considered ‘misconduct’ under the SFO, potentially resulting in disciplinary action by the SFC.

For the HKCC, with its leadership bringing enforcement experience from the United States and the European Union, and following the aforementioned favourable rulings from the Competition Tribunal in 2019 and 2020, the HKCC is likely to continue the momentum in enforcement action by bringing high-profile enforcement actions in 2020 and beyond. As for the type of cases, while all six enforcement actions the HKCC has taken so far have targeted cartel conduct, Mr Brent Snyder, chief executive officer of the commented in April 2019 that the HKCC were prepared to take enforcement action against non-cartel cases and had a diverse range of ongoing investigations including those under the Second Conduct Rule and non-cartel contraventions of the First Conduct Rule. These violations, however, are harder to pursue, as complex economic analysis is needed, which will require the HKCC to devote more resources to its investigations.

70 For example, Chinese e-commerce giant Alibaba, with an existing primary listing on the New York Stock Exchange, achieved a secondary listing in Hong Kong in November 2019.
71 See footnote 61.
72 In 2017, the HKCC appointed Mr Brent Snyder as chief executive officer, formerly Deputy Assistant Attorney General at the US Department of Justice, and Mr Jindrich Kloub as executive director (operations), formerly an official of the Directorate General for Competition at the European Commission.
74 The Second Conduct Rule prohibits an undertaking that has a substantial degree of market power in a market from abusing that power by engaging in conduct that has as its object or effect the prevention, restriction or distortion of competition in Hong Kong. See Section 21 of the Competition Ordinance (Cap. 619).
75 See footnote 23.
Nonetheless, companies are reminded to obtain sound legal advice to better understand evolving legal practice in this area and secure protection in current or potential investigations. The most recent four enforcement actions, all involving penalties sought against individuals, also mark its vision to continue to take actions on not just companies but also individuals. According to the HKCC, insofar as the HKCC may take action against individuals who are involved in anti-competitive conduct, its priority will be to focus on those involved who are part of the management of the company under investigation or who otherwise directed the cartel conduct, rather than frontline staff who followed their directions.76

I INTRODUCTION

In India, there are several authorities and agencies that have been empowered to investigate and prosecute illegal corporate actions. All law enforcement agencies, such as the local police, the Central Bureau of Investigation (CBI), the Enforcement Directorate (ED) and the Serious Fraud Investigation Office (SFIO) are empowered to investigate and prosecute companies. The SFIO is the primary agency to investigate and prosecute corporate frauds. The ED investigates and prosecutes cases related to foreign exchange regulation violations and money laundering. The CBI investigates and prosecutes cases related to corruption, financial frauds, bribery and the like. The Income Tax Department investigates and prosecutes cases related to income tax violations. The local police investigate and prosecute companies for offences under the Indian Penal Code (IPC) and other industry specific statues, such as the Food Safety and Standards Act 2006.

The powers of the investigating agencies are regulated by the Code of Criminal Procedure 1973 as well as specific statutes from which they may derive their powers. Moreover, practice guidelines published by investigative agencies also seek to regulate their powers. The powers of these agencies are wide-ranging in nature and pertain to collection of information, investigation, search and seizure, and detention. Investigative agencies, such as the CBI can conduct ‘dawn raids’. However, these dawn raids require a valid search warrant.

All agencies have similar (if not identical) powers to investigate; namely, the power to collect information, conduct search and seizure operations, detain suspected individuals and conduct dawn raids. Some specialised law enforcement agencies enjoy certain enhanced powers. The ED has much wider powers to attach assets during the course of investigation, if it has reason to believe that any asset has been acquired from proceeds of crime. Additionally, the National Investigation Agency (NIA) when investigating offences affecting national security, sovereignty and interests of India, has the power to directly make arrests in different states, without the assistance of or without informing the concerned state agencies.

Though the investigations and prosecutions conducted by these agencies are required to be impartial and uninfluenced by extraneous considerations, there have been instances when these investigations have been motivated by political agendas. Therefore, it is advisable for any corporate entity being the subject of any investigation, to extend its cooperation to the investigating agencies and provide all information, documents and evidence, as may be sought. While the company may want to resist a request
for information or documents on grounds of relevance and reasonableness, it may result in the company appearing as non-cooperative. Both prosecutors and Indian courts appreciate cooperation during an investigation and an adversarial stance may result in tougher actions from both investigators and courts, resulting in business disruptions. Having said that, Indian courts are sympathetic to genuine challenges on jurisdiction of an investigation agency, challenges to a fishing and roving enquiry. The thresholds of judicial intervention at early stages of an investigation may be less.

II CONDUCT

i Self-reporting

In India, the law in general does not mandate any corporate entity to self-report any internal wrongdoing and the option of whether or not to report the same to the investigating agencies completely vests with the corporate entity. Also, self-reporting of internal wrongdoing is neither considered a mitigating factor in determining liability, nor does it entitle the corporate entity to any immunity or leniency in prosecution.

Sanctions for violation of competition law are governed under the Competition Act 2002 (Competition Act). Section 3 of the Competition Act prohibits anticompetitive agreements that cause or are likely to cause an appreciable adverse effect on competition (AAEC) in India and treats these as void. Such agreements include cartels, which are presumed under the Competition Act to have an AAEC.

In cases where a firm is found to be participating in a cartel, a penalty of up to three times the profit of the participating firm for each year of the continuance of the cartel or 10 per cent of its relevant turnover for each year of continuance of the cartel, whichever is higher, can be imposed on the company as well as on every person who, at the time the contravention was committed, is in charge of and responsible to the company. In addition, the Competition Commission of India (CCI) can direct the participating firm to cease and desist from engaging in anticompetitive conduct.

Voluntary disclosure by companies engaging in AAEC attracts leniency from the CCI in the amount of penalties. The CCI is empowered to grant to an enterprise a reduction in penalty of up to 100 per cent in cases where the CCI, without the disclosure by the enterprise, would not have had sufficient evidence to establish the contravention. Also, the CCI is empowered to grant a reduction in penalty of up to 50 per cent and 30 per cent to the second or third enterprises, respectively, who make a disclosure while being a part of the cartel, by submitting evidence that provides a significant added value to the evidence already available with the CCI or Director General for establishing the existence of the cartel.

That being said, the CCI has no jurisdiction to impose criminal sanctions on companies for cartel violations under the Competition Act. The only situation where the Competition Act allows for criminal sanctions is on contravening the orders of the CCI or on failure to pay the penalties imposed. Such non-payment is punishable by imprisonment for a maximum term of three years, a maximum fine of 250 million rupees, or both. Additionally, the National Company Law Appellate Tribunal has the power, similar to that of the High Court, to punish conduct in contempt of its orders, and can specifically impose criminal sanctions, in the nature of both fines and imprisonment, for contempt of its orders.

2 Competition Commission of India (Lesser Penalty) Regulations 2009.
ii Internal investigations

A company is at liberty to decide whether or not to conduct an internal investigation and the same is neither mandatory under Indian law nor is it regulated by any legislation. However, a corporate entity, in order to fulfil its statutory or regulatory obligation under the Sexual Harassment of Women (Prevention, Prohibition and Redressal) Act 2013, Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015 and the provisions relating to internal controls and audits in Companies Act 2013, may choose to conduct an internal investigation in compliance with its legal and regulatory requirements.

There is no obligation on any corporate entity to share the reports or result of the internal investigations with the investigating agencies and, even if submitted, the results of the internal investigation are not binding on the investigating agencies. Submission of these reports is at best a gesture of good faith and cooperation by companies. That being said, the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015, requires listed companies to make disclosures to the stock exchanges of any events or information such as fraud, etc., which, in the opinion of its board of directors, is material.

There is no legal framework to regulate the conduct of internal investigations. As such, the companies and external counsel engaged for conducting the internal investigation are at liberty to determine the procedure for the same. Such investigations may involve either document review or witness interviews or both. Further, there is no prescribed procedure for conducting the witness interview of an employee and there is no legal requirement that mandates an employee to have legal representation at the interview. On rare occasions, employees (especially senior management) or other key managerial personnel do insist on the presence of their own lawyer. That being said, companies usually engage external counsel to conduct investigations with the protection of attorney–client privilege.

Companies generally engage external counsels to conduct internal investigations, keeping in mind the aspect of preserving privilege over the work product generated during the investigation. Even though attorney–client or work product privileges can be asserted in internal investigations, this privilege can be waived by the company in cases where it may disclose the findings and supporting material to law enforcement agencies. While this remains judicially untested, disclosure of investigation findings or material to law enforcement is likely to be considered to be a waiver of privilege.

iii Whistle-blowers

Whistle-blower complaints to government authorities and corporates in India have been on the rise in recent years. However, despite the increase in instances of whistle-blower complaints in recent times, no incentives are provided to the whistle-blowers under the legislative framework to come forward and ‘red flag’ issues.

The Whistle Blowers Protection Act 2014 (WPA 2014) is a statute seeking to regulate receipt, disclosure and protection of whistle-blowers. While the WPA 2014 has indeed been passed by the parliament, it is yet to be notified and therefore has not been implemented or operationalised into law in India.

Under the Companies Act 2013, every listed company is required to establish a vigil mechanism for its directors and employees to report genuine concerns and penalties are imposed on companies that fail to comply with this requirement. The existence of such a mechanism is also required to be disclosed in the report of the Board of Directors.
the Companies Act 2013 requires independent directors to ascertain whether the company has an adequate and functional vigil mechanism as well as ensuring that the interests of persons who use such mechanisms (whistle-blowers) are protected. Also, the Securities and Exchange Board of India (SEBI) corporate governance rules require companies to establish a functional whistle-blowing mechanism and ensure adequate protection to whistle-blowers.

The Companies Act 2013 and its allied rules, without being specific as to the nature and extent of the safeguards required, mandates that the vigil mechanism put in place by the company shall ensure adequate safeguards against victimisation of the whistle-blower.

III ENFORCEMENT

i Corporate liability

Generally, under Indian criminal law, corporate criminal liability is established through the principle of attribution of intent. The criminal intent of the individuals (directors, agents or employees) representing the directing mind or alter ego of the company is attributable to the company to hold the company liable along with the individuals. Therefore, criminal liability is imputed to the company when the directors, agents, etc. of the company act with criminal intent in the course of the business of the company. As a matter of law, this principle cannot be applied in reverse in the absence of a specific statutory provision imposing vicarious liability (as discussed above). Therefore, directors and agents of a company cannot be subject to criminal liability, in the absence of any involvement or intent on their part, merely because criminal liability attaches to the company. Certain statutes, through specific provisions, hold individuals liable for offences committed by a company (vicarious liability); for example, the Negotiable Instruments Act 1881, provides that the directors of a company can be held liable along with the company in cases where a cheque issued by a company is not honoured.

Civil liability of corporations for conduct of their employees flow through well-established common law principles of vicarious liability (i.e., companies are vicariously liable for the actions of their employees conducted in the course and for the purposes of their employment).

Joint representation of the corporation and individuals is not expressly forbidden under Indian law. It is permissible for corporations and individuals to be represented and advised by the same counsel so long as their positions are not adversarial. Such joint representation may also be permissible when statutory vicarious criminal liability is imputed to the individuals in question. However, it is advisable for the corporation and the individuals to retain different counsel. This acts to mitigate potential issues of conflict of interest and attorney client privilege. Moreover, the course of a criminal trial and investigation is unpredictable and may result in the corporation and the individual becoming adversarial, even if they were not initially so. Therefore, it is recommended that that corporations and individuals retain separate counsel.

ii Penalties

The range of sanctions available against businesses includes:

a Fines – the amount of fine levied depends on the specific nature of the offence and the facts of the case. Whether the fines in nature are administrative or criminal will depend on the specific statute or provisions under which the fines are levied. For instance, fines
for non-compliance of filing requirements under the Companies Act 2013 would be administrative in nature. However, fines levied post a trial under the Prevention of Corruption Act 1988 (POCA) would be criminal in nature.

b Imprisonment of concerned company officials – the duration of the imprisonment depends on the nature of the offences, as well as the specific conduct of the individuals involved as well as other facts of the case.

c Regulatory or civil sanctions – regulatory sanctions in the nature of cancellation of industry sector-specific licences (electricity, telecom, etc.) can be imposed by various regulatory bodies for violations of regulatory norms, including terms requiring compliance with applicable law and anti-bribery obligations.

Civil sanctions in the nature of blacklisting from public tenders can also be levied by government bodies if a bidder has engaged in fraudulent or corrupt practices generally during the bidding process, or in past experiences with the same government entity. The SEBI has powers to punish persons and corporations engaging in fraudulent and unfair trade practices in relation to the securities market by levying restrictions on their operations in the market.3

iii Compliance programmes

The existence of a compliance programme can serve as a defence to specific criminal charges brought under India’s anti-bribery legislation – the POCA.

Specifically, under Section 9 of the POCA, a new offence of ‘bribing of a public servant by a commercial organisation’ was introduced, providing that if any person ‘associated with a commercial organisation’ (defined to mean any person performing services for or on behalf of such organisation including an employee, agent or subsidiary) gives or promises to give any undue advantage to a public servant intending to (1) obtain or retain business for such organisation or (2) obtain or retain an advantage in the conduct of business of such organisation, then such commercial organisation (including a company incorporated within India, or outside India and carrying on business in India) shall be punishable with a fine. The officers and directors of the company involved in the offence can also be punished with imprisonment and a fine.

While commercial organisations are allowed to raise a defence that they had adequate procedures (in compliance of prescribed guidelines by the government) in place to prevent acts of bribery punishable under the POCA by their ‘associated person or persons’, the government is yet to notify these ‘prescribed guidelines’.

In the lack of clarity from the government on the contents of these prescribed guidelines, companies would be best served to adopt compliance programmes in line with international best practices.

Moreover, this defence is specific to offences under the POCA and does not extend to offences under other legislations, including offences under the Indian Penal Code 1860 (IPC).

**iv Prosecution of individuals**

There are no legal rules that seek to regulate the relationship between the company and individuals, when the government seeks to hold the individuals liable. However, this is a sensitive issue that has to be appropriately navigated by the company, keeping in mind the nature of allegations, the investigative agency involved, as well as the potential reputational risk. The company will have to ensure that the cooperation and assistance provided to the individual does not give an impression of collusion to the investigating agency. Additionally, the company must keep in mind issues of conflict of interest and the potential for the company’s and individual’s position to become adversarial during the course of the investigation or trial.

Keeping in mind the foregoing, the company’s counsel can coordinate with the individual’s counsel and there is no specific bar on the company paying the individual’s counsel or legal fees. There is no obligation for the company to either terminate or discipline the employees who are subject to the investigation. The company retains its liberty to terminate or discipline the individuals in question according to their existing policies, the nature of allegations and the reputational risk involved.

**IV INTERNATIONAL**

**i Extraterritorial jurisdiction**

The IPC grants extra-territorial jurisdiction to Indian courts in the following circumstances:

- offences committed by Indian citizens, persons, ships or aircrafts can be prosecuted under Indian courts even if the offence is committed outside of India, provided the offence would be punishable in India had it been committed there;4

- offences by non-citizens (including foreign companies) can be prosecuted and punished in India provided that these extra-territorial criminal acts are made expressly punishable by Indian laws;5 and

- any person (including foreign companies) in any place outside India can be prosecuted and tried before Indian courts for the offence of targeting a computer resource located in India.6

Additionally, under the Prevention of Money Laundering Act 2002 (PMLA), the ED has the power to attach property located in foreign states that is derived from or obtained directly or indirectly as a result of criminal activity set out in the schedules of the PMLA. Moreover, such properties can also be attached under the Fugitive Economic Offenders Act 2018 (Fugitive Act) provided the total value of the offence is more than 1 billion rupees.

**ii International cooperation**

The Indian government cooperates with other countries’ law enforcement. This cooperation is primarily treaty based, but cooperation can also be sought through diplomatic channels. India has entered into mutual legal assistance treaties (MLAT), with 39 foreign nations for the purpose of ensuring service of summons, warrants and judicial processes to individuals.

---

4 Section 4(1) and (2) of the IPC.
5 Section 3 of the IPC.
6 Section 4(3) of the IPC.
or entities believed to be involved in the commission of crimes. India is also a party to the Financial Action Task Force to cooperate and coordinate global and international anti-money laundering efforts.

India extradites its own nationals, as well as foreign nationals, but the frequency is not certain. The government of India has also entered into bilateral extradition treaties with 42 countries and has entered into extradition arrangements with 11 more, pursuant to the provisions of the Indian Extradition Act 1962. The circumstances in which extradition is possible differs from case to case, as well as treaty to treaty. Broadly, extradition is possible when the following conditions are met, and a request is made to the Consular, Passport and Visa Division, Ministry of External Affairs:

- extradition applies only with respect to offences clearly stipulated in the respective treaties;
- the offence for which extradition is sought is an offence under the laws of both the requesting country and India;
- India must be satisfied there is a prima facie case against the accused;
- the extradited person must be proceeded against only in respect of the offence for which extradition is requested; and
- the extradited person must be accorded a fair trial.

Provisional arrest requests from any foreign state may be made to India, irrespective of any treaty requirements.

iii Local law considerations

While banks have a duty of secrecy to customers in India, it is not an absolute duty. Courts have the power to direct disclosure of details of accounts under the Bankers’ Books Evidence Act 1881. Investigative agencies also have the power to ask for production of statement of accounts from banks during the course of the investigation. Therefore, it is likely that bank secrecy laws would not be a significant obstacle to obtaining information in the course of a multi-jurisdiction investigation.

Indian data privacy laws are nascent and are in the process of being developed. Disclosure of sensitive personal information (which includes data such as passwords, bank account or credit card details, physical, physiological and mental health data, biometric information) requires consent of individuals prior to sharing such information by organisations in possession of such information. However, this information can be provided to law enforcement agencies without prior consent, upon the receipt of a written request. Therefore, it is likely that data privacy laws will not be a significant hurdle to obtaining information during multi-jurisdiction investigations.7

While attorney client privilege may be recognised in case of communication with external local counsel, the benefit of this protection does not extend to in-house attorneys or foreign counsel.

---

7 See the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
V YEAR IN REVIEW

The Fugitive Act was introduced in 2018. It is India’s newest criminal statute. However, active prosecution under the Fugitive Act is already underway. Diamantaires Nirav Modi and Mehul Choski, who are allegedly involved in a bank fraud involving 3 billion rupees and have since absconded from India, are being prosecuted under the Fugitive Act. Nirav Modi was declared as a Fugitive Economic Offender under the provisions of the Fugitive Act in November 2019. An application for release of confiscated assets was moved by the aggrieved. The decision on this is awaited from the court. This will be the first decision on issues of confiscation under the Fugitive Act. There are several important questions of law involved and the decision in this matter will lay the foundation for the interpretation of this criminal statute.

The Indian government is adopting a tougher position against corporate frauds. New amendments to the Companies Act 2013 were recently notified. These amendments enable the SFIO to identify the beneficiaries of a corporate fraud and initiate legal action for disgorgement of these benefits. Prosecution of corporate fraud cases by the SFIO, including the production of the arrested and accused persons will now take place in special courts. Following the amendments, there has been a significant uptick in investigations, arrests, searches, etc. by the SFIO. The SFIO is actively investigating various high-profile corporate fraud cases in India, despite the lockdown as a result of the covid-19 pandemic in India, such as the alleged fraud involving the ILFS Group and an alleged bank fraud involving 7.5 billion rupees by the promoters of the Rotomac Group.

Moreover, the Ministry of Corporate Affairs has mandated additional fraud reporting requirements by companies in their Auditor’s Report by way of the Companies (Auditor’s Report) Order 2020 (CARO) after consultation with the National Financial Reporting Authority. This order prescribes the following insertions into the Auditor’s Report:

\[a\] whether any fraud by or on the company has been noticed or reported during the year; if yes, the nature and the amount involved is to be indicated;

\[b\] whether any report under Section 143(12) of the Companies Act 2013 (Auditor’s obligation to report incidents of fraud to the central government) has been filed by the auditors in the prescribed form;\(^8\) and

\[c\] whether the auditor has considered whistle-blower complaints, if any, received during the year by the company.

VI CONCLUSIONS AND OUTLOOK

It appears that the Indian government is adopting a tougher stance against corporate frauds and corruption. This is evident from the ramping up of investigations by the SFIO and other law enforcement agencies, and from regulatory changes such as the CARO. This tougher approach is also evident from the amendments to the POCA seeking to criminalise bribe-giving by individuals and corporations.

Additionally, India has been in a covid-19-related lockdown for two months as at time of writing. This situation carries an increased risk of bribery within India. Government-mandated lockdowns seek to regulate which businesses can remain operational and the limitations of their functioning. Moreover, policies regulating the functioning of specific industry sectors

---

\(^8\) Form ADT-4 as prescribed under rule 13 of Companies (Audit and Auditors) Rules 2014
may require further government interaction. This, naturally, becomes a risk factor for anti-corruption compliance. Third parties and intermediaries used by companies may seek to sidestep some regulations through bribery of government officials. Further, given that a significant part of the resources and attention of the company will be directed towards addressing business challenges, companies will also face an enhanced risk of financial fraud during this time. As with potential anti-corruption compliance violations, there is a significant risk that internal frauds committed during this time may not be discovered until much later.

As a result, it is likely there will be an increase in the number of investigations surrounding corruption and fraud in the aftermath of the covid-19 lockdowns. This will result in a challenging climate both for law enforcement agencies as well as the companies involved, in the short term.
Chapter 15

IRELAND

Karen Reynolds and Ciara Dunny

I INTRODUCTION

Generally, Ireland is considered a low-risk economy and a secure place in which to do business. In January 2020, Transparency International published its 2019 Corruption Perceptions Index, which measures the perceived levels of public sector corruption in 176 countries. In 2019, Ireland ranked 18th with a score of 74. According to the index, Ireland continues to be perceived as one of the least corrupt countries in the world. However, in spite of this, Ireland has been criticised following the financial crisis for its lack of enforcement in the areas of corporate governance and white-collar crime, and Transparency International’s 2018 Progress Report assessing enforcement of the OECD’s Anti-Bribery Convention ranked Ireland as conducting ‘little or no enforcement’ of the convention.

In November 2017, the Irish government published the Measures to Enhance Ireland’s Corporate, Economic and Regulatory Framework, aimed at strengthening Ireland’s response to corporate misconduct. The focus of the framework is combating white-collar crime and has been developed to augment the existing regulatory and legislative framework in the area of corporate, economic and regulatory crime. The measures are a further commitment by the government to ensure Ireland is a secure place in which to do business. Since their publication, a number of these measures have been introduced, such as the enactment of the Criminal Justice (Corruption Offences) Act 2018 on 30 July 2018, which effectively repealed and replaced the seven existing Prevention of Corruption Acts 1889 to 2010 with one statute.

In addition, the Law Reform Commission’s Report on Regulatory Powers and Corporate Offences was published in October 2018, and this recommended a number of reforms, such as:

a the establishment of a sufficiently resourced and multidisciplinary statutory Corporate Crime Agency;

b the introduction of deferred prosecution agreements;

c a core set of regulatory powers for all regulators in the wider economic context, such as in competition law, communications regulation and health products regulation, including the power to impose administrative sanctions and compliance settlements; and

d a reformation of fraud offences to include liability for ‘subjective recklessness’.

Karen Reynolds is a partner and Ciara Dunny is a senior associate at Matheson.


ibid.
The Law Reform Commission also set out a number of recommendations for corporate offences that would clarify the circumstances in which a corporate body could be held criminally liable for systemic failures by its senior executives.

There has been a significant increase in regulatory oversight and enforcement in Ireland in recent years. The Irish Data Protection Commission (DPC) is now one of the best resourced data protection authorities in Europe, with huge investment in industry experts, and investigations launched into 19 multinational technology companies during 2019. The Central Bank, Ireland’s primary financial services regulator, continues to take a strong line on the conduct and culture of the firms it regulates, promoting greater individual accountability and taking a strong line on enforcement. It has imposed 134 fines on regulated entities under its Administrative Sanctions Procedure, bringing total fines imposed by the Central Bank since 2006 to over €103 million. The Office of the Director of Corporate Enforcement (ODCE) in Ireland has also recently launched a number of high-profile investigations into corporates for matters relating to corporate governance.

There are a number of bodies, regulatory and otherwise, empowered to investigate corporate conduct in Ireland, including:

a. An Garda Síochána (the Irish police);

b. the ODCE;

c. the Office of the Revenue Commissioners (the Revenue Commissioners);

d. the Central Bank; the Competition and Consumer Protection Commission (CCPC);

e. the DPC;

f. the Health and Safety Authority (HSA);

g. the Commission for Communications Regulation (ComReg);

h. Customs and Excise;

i. the Criminal Assets Bureau;

j. the Environmental Protection Agency;

k. the Health Products Regulatory Authority;

l. the Health Information and Quality Authority; and

m. the Workplace Relations Commission.

Offences are either summary (minor) or indictable (serious). In general, regulatory bodies are authorised to prosecute summary offences. However, the Office of the Director of Public Prosecutions (DPP) is the relevant body for the prosecution of criminal offences on indictment. The DPP has no investigative function; the relevant regulatory or investigating body prepares a file and submits it to the DPP for consideration. It is then solely at the discretion of the DPP as to whether a case will be taken in respect of the suspected offence.

The investigation of criminal offences is primarily the function of the police. The police have a wide range of powers, which include:

a. to approach any individuals and make reasonable enquiries to stop and search;

b. to seize evidence;

c. to enter and search premises; and

d. to detain and arrest.

There are a number of specialist units that support the police with investigations into corporate misconduct, including the Garda National Economic Crime Bureau (GNECB), the Criminal Assets Bureau (CAB) and the Garda National Cyber Crime Bureau (GNCCB). The GNECB investigates economic crime, including fraud, the CAB investigates the suspected proceeds of
criminal conduct and the GNCCB is tasked with the forensic examination of electronic data seized during the course of criminal investigations in addition to conducting investigations into cyber crime or online offences.

Currently, the ODCE is afforded a wide range of investigative powers under the Companies Act 2014 and is responsible for the enforcement of company law, including:

- by way of fact-finding investigations;
- prosecutions for suspected breaches of company law;
- supervision of companies in official and voluntary liquidation and of unliquidated insolvent companies;
- restriction and disqualification of directors and other company officers; and
- the regulation of undischarged bankrupts acting as company officers.

In respect of prosecution, the ODCE has the power to prosecute summary offences and to refer cases to the DPP for prosecution on indictment. However, under the General Scheme of the Companies (Corporate Enforcement Authority) Bill 2018, which was published in December 2018, it is proposed that the ODCE will be re-established as an agency, in the form of a commission, which will be known as the Corporate Enforcement Authority (CEA). The CEA will be established as an independent company law compliance and enforcement agency, and will have greater powers than the ODCE. The CEA will operate independently of any government department to provide more independence in addressing company law breaches. The establishment of the CEA is regarded as a fundamental element of the government’s commitment to enhance Ireland’s ability to combat white-collar crime.

The primary function of the CEA will be to encourage compliance with the Companies Act 2014. As such, its role will be to investigate instances of suspected offences or non-compliance with the Companies Act 2014. This may involve the appointment of inspectors, the commencement of criminal investigations and the resulting prosecution of summary offences, together with the civil enforcement of obligations, standards and procedures. The Bill also seeks to give the CEA new investigative tools. First, it provides for the admission of written statements into evidence in certain circumstances and will create a statutory exception to the rule against hearsay. Second, there is an enhanced power regarding the searching of electronically held evidence in that the CEA will be permitted to access data under the control of an entity or individual, regardless of where the data is stored and to access it using any means necessary to ensure best compliance with evidence rules and digital forensics principles.

The Central Bank also has investigatory and regulatory powers, including powers of inspection, entry, search and seizure, in respect of financial institutions under the Central Bank Act 1942, as amended. The Central Bank is responsible for regulating the financial services industry. Its enforcement work can be divided into two processes: an administrative sanctions procedure by which the Central Bank investigates breaches of financial services law by regulated firms and individuals; and a fitness and probity regime pursuant to which individuals in designated positions within regulated firms must be competent, capable, honest, ethical, of integrity and financially sound. The Central Bank’s investigative powers include compelling the production of documents, compelling individuals to attend interviews and conducting on-site inspections. The Central Bank publishes its Strategic Plan.

---

4 Section 949(c) and (d) of the Companies Act 2014.
every three years, which sets out its priorities for the next three-year period based on a set of strategic themes and their statutory and organisational objectives. In its current Strategic Plan 2019–2021, it lists the following themes as its strategic objectives: strengthening resilience; Brexit; strengthening consumer protection; engaging and influencing; and enhancing organisation capability.

The Revenue Commissioners is the government agency responsible for the assessment and collection of taxes. It also has investigative and prosecutorial powers to:

- enter and search premises;
- inspect goods and records;
- take samples;
- question individuals;
- remove and retain records;
- stop, search and detain vehicles;
- seize and detain goods and conveyances; and
- search and arrest individuals.

The investigation and prosecutions division is responsible for the development and implementation of policies, strategies and practices in relation to serious tax evasion and fraud offences. It has a wide range of powers, which include: to conduct civil investigations; to conduct investigations into trusts and offshore structures, funds and investments; and to obtain High Court orders. Of particular significance is the power to obtain information from financial institutions and procure search warrants to this effect.

The CCPC is responsible for enforcing competition and consumer protection law and holds extensive powers of investigation in relation to suspected breaches of competition and consumer protection law. The CCPC has powers of entry and search and seizure, including the power to search any premises used in connection with a company. Its search powers are not confined to a company's offices but extend to the homes of directors or employees. The CCPC's powers extend to compelling evidence and individuals, powers recently utilised during its ongoing investigation in the motor insurance sector in Ireland.

ComReg is responsible for the regulation of the telecommunications industry and is one of the more prolific regulatory enforcers in Ireland, with wide ranging powers of investigation, including powers to compel evidence, powers of entry and search and seizure, and the power to levy fines through applications to the Irish courts.

The regulatory body previously known as the Office of the Data Protection Commission is now known as the DPC under the Data Protection Act 2018. It is responsible for upholding the fundamental right of individuals to data privacy through the enforcement and monitoring of compliance with data protection legislation in Ireland. If the DPC receives a complaint relating to a breach of data protection rights, it is obliged to investigate the alleged breach, though it will generally require the complainant to raise the matter directly with the organisation concerned in the first instance. Additionally, the DPC may investigate the unlawful processing of personal data and audit data processors of its own accord. The DPC

---

5 Section 899 of the Taxes Consolidation Act 1997.
6 ibid., Section 895.
7 ibid., Sections 902A and 908.
8 ibid., Section 908C.
9 Section 36 of the Competition and Consumer Protection Act 2014.
secures compliance with data protection law through the exercise of its statutory powers, including the use of enforcement notices. It is an offence for a controller or processor to fail to comply with an enforcement notice without reasonable excuse. In May 2020, the child and family agency, Tusla, was the first organisation to be fined by the DPC for a breach of The General Data Protection Regulation 2016 (GDPR). It was fined €75,000 arising out of an investigation into three cases where information about children was wrongly disclosed to unauthorised parties.

The HSA is responsible for ensuring that workers are protected from work-related injury and ill health by enforcing occupational health and safety law. The powers of the HSA include the right of entry, the right of inspection, the right to require the production of records, the right to require the provision of information, the right to take measurements and samples, and the right to require that machinery be dismantled.

The DPP was created by statute with the specific aim of maintaining prosecutorial independence. Section 6 of the Prosecution of Offences Act 1974 makes it an offence for persons (other than an accused, suspect, victim or person directly involved) to communicate with the DPP with a view to influencing a decision to commence or continue criminal proceedings. However, arguably there is a lack of transparency in relation to the decisions to prosecute, or not prosecute, particular crimes, as the DPP does not publish the reasons for a decision on prosecution. The DPP introduced a pilot scheme on 22 October 2008, under which the DPP will publish the reason for its decision not to prosecute in cases where an individual has died as a result of an alleged crime, including manslaughter and workplace death. For all decisions made on or after 16 November 2015, a victim can ask the DPP for a summary of the reasons for its decision.

Investigating authorities may request companies in Ireland to assist them in their investigations on a voluntary basis. There are specific provisions pursuant to which regulatory and law enforcement authorities can compel cooperation or participation of a company or individual; however, these provisions are often not exercised at least in the first instance. Companies and individuals should be cognisant of contractual obligations of confidentiality and the rights of privilege against self-incrimination if any such request is made by any regulatory or law enforcement authority.

II CONDUCT

i Self-reporting

There are a number of legislative provisions that impose a positive obligation on persons (including companies) to report wrongdoing in certain circumstances:

a Section 19 of the Criminal Justice Act 2011 (the 2011 Act) provides that a person is guilty of an offence if he or she fails to report information that they know or believe might be of material assistance in preventing the commission of, or securing the prosecution of, another person of certain listed offences, including many white-collar offences. The disclosure is required to be made as soon as is practicable. However, the person considering making the report may need to make enquiries to be satisfied that a report is justified. The applicable standard for what information meets the threshold of ‘material assistance’ in preventing the commission of, or securing the prosecution of,
an offence has not yet been expanded on or tested before the Irish courts. However, in the Supreme Court decision of *Sweeney v. Ireland*, the court saw a challenge to the constitutionality of a nearly identical offence under Section 9(1) of the Offences Against the State (Amendment) Act 1998. The wording of Section 19(1)(b) of the 2011 Act is identical to that of Section 9(1)(b) of the 1998 Act except that the former applies to a ‘relevant offence’ and the latter applies to a ‘serious offence’. In finding that the provision was sufficiently certain, the Supreme Court held that the 1998 Act was clear in what it obliges witnesses to do: to disclose information pertaining to serious offences that they know will aid in the prosecution of such an offence. The judgment also discussed the similar reporting obligation under Section 19 of the Criminal Justice Act 2011, among others, and while the court noted that no comment has been made as to the constitutionality of such similar provisions, the decision provides clarification that such reporting obligations would likely withstand any legal challenge and thus trigger criminal offences if not complied with.

The relevant offences for the purposes of the 2011 Act are specified in Schedule 1 of the 2011 Act and include offences under the Criminal Justice (Corruption Offences) Act 2018. As a result, it imposes a mandatory obligation on both companies and individuals to report suspected instances of bribery and corruption. However, no specific statutory provision exists in Ireland providing for leniency where a company self-reports a corruption or bribery offence.

Section 38(2)(a) of the Central Bank (Supervision and Enforcement) Act 2013 places an obligation on the senior personnel of a regulated financial services body to disclose to the Central Bank of Ireland (CBI), as soon as is practicable, information relating to a suspicion of, or the commission of, an offence under financial services legislation.

Section 42(1) of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended provides that certain designated persons have an obligation to report any knowledge or suspicion that another person has been or is engaged in an offence of money laundering or terrorist financing to the police and the Revenue Commissioners.

Section 59 of the Criminal Justice (Theft and Fraud Offences) Act 2001 obliges the auditor of a company to disclose to the police information of which the auditor may become aware in the course of his or her duties that suggests the commission by the company or entity of any offences under that Criminal Justice (Theft and Fraud Offences) Act 2001. This obligation is notwithstanding any professional obligations of privilege or confidentiality on the part of the auditor.

Section 393 of the Companies Act 2014 as amended places a duty on auditors to report to the ODCE where an auditor comes into possession of information that leads him or her to believe that a Category 1 or 2 offence may have been committed. The Companies Act 2014 sets out the different types of offences by categorising them from 1 to 4, with Category 1 being the most serious. Category 1 offences include offences such as false accounting and fraudulent trading. Category 2 offences range from financial assistance, dishonest dealings before a company becomes insolvent or goes into liquidation, failure to keep adequate accounting records, failure to communicate with and make full disclosure to statutory auditors and other similar offences.
Although, in practice, self-reporting may be a mitigating factor in prosecution or sentencing, immunity or leniency based on this conduct is rarely expressly afforded by legislation. However, the list of sanctioning factors set out in the CBI’s Administrative Sanctions Procedure includes ‘how quickly, effectively and completely the regulated entity brought the contravention to the attention of the CBI or any other relevant regulatory body’.12

The DPP has a general discretion whether to prosecute in any case having regard to public interest. Within that discretion is the power to grant immunity in any case. Any grant of immunity will generally be conditioned on the veracity of information provided and an agreement to give evidence in any prosecution against other bodies or individuals. There are no specific guidelines governing the granting of immunity in general. However, in the realm of competition law, the CCPC, in conjunction with the DPP, operates a Cartel Immunity Programme (CIP) in relation to breaches of the Competition Act 2002, as amended. Applications for immunity under the CIP are made to the CCPC. However, the decision to grant immunity is ultimately at the discretion of the DPP.

A person applying for immunity under the CIP must come forward as soon as possible and must not alert any remaining members of the cartel to their application for immunity under the programme. Further, the applicant must not have incited any other party to enter or participate in the cartel prior to approaching the CCPC. Immunity under the CIP is available only to the first member of a given cartel who satisfies these requirements.

Once an application for conditional immunity has been granted, a positive duty is imposed on the applicant to cooperate fully with the investigation, on a continuing basis and at no expense to the CCPC. In particular, the applicant must reveal all cartel offences in which he or she was involved and provide full disclosure in relation to same. If the applicant is a company or corporation, the application for immunity must be made by the company in its separate legal capacity. Failure to comply with the requirements set out in the CIP may result in conditional immunity being revoked by the DPP.

### ii Internal investigations

There is generally no restriction on a company initiating an internal investigation, particularly in relation to suspected criminal conduct. The company is only under an obligation to share the results of an investigation with the relevant authorities where it is required under a court order, statute or self-reporting obligation (see Section II.i). In considering such matters, the advice of external legal counsel is usually engaged.

An internal investigation usually makes use of a wide range of evidence; hard-copy and electronic documentation, witness interviews, computer forensics and financial records are all open to an internal investigation.

There has been some clarification of issues surrounding fair procedures in recent case law. In *Joyce v. Board of Management of Colaiste Iognáid*, the High Court held that natural justice principles do not apply at the initial stages of an investigation, such as the initial consideration of an issue, but are engaged when formal proceedings from which findings may be drawn commence.13

If witness interviews are conducted, the employees in question have no statutory right to legal representation. However, if an employee or witness is, or may become, the subject

---

of the investigation, the employer should consider advising the employee or witness to have legal representation to be sure of being afforded fair procedures rights and to prevent any later legal challenge to the investigation process. However, this should be assessed case by case.

Any requirement to disclose documents obtained through an internal investigation to the authorities is qualified by legal professional privilege. Documentation may attract legal professional privilege, either in the form of legal advice privilege or litigation privilege. Legal advice privilege protects from disclosure any confidential communications between a lawyer and his or her client created for the purpose of seeking, giving or obtaining legal advice. In *Miley v. Flood*, the High Court confirmed that legal professional privilege can only be invoked in respect of legal advice and not in respect of legal assistance. Litigation privilege, which is broader than legal advice privilege, applies to confidential communications between a lawyer and a client, or one of them and a third party such as an expert, the dominant purpose of which is for use in contemplated or existing litigation.

In the decision in *Re Sean Dunne (a bankrupt) v Yesreb Holding & anor: Celtic Trustees v Sean Dunne (a bankrupt)*, the Irish courts adopted a narrow view regarding the purpose for which a document was created during an investigation. The court found that litigation privilege did not attach to the transcript of an interview carried out by the official assignee with one of the vendors of a property that had been purchased by Sean Dunne, as the dominant purpose of the interview was for investigation rather than the conduct of litigation, though it was accepted that litigation was apprehended at the time of the interview. However, the refusal to recognise the transcript as privileged may have stemmed from the particular facts of the case and the fact the investigation was carried out under a statutory investigative order.

In another recent decision of the Irish High Court in *Director of Corporate Enforcement v. Buckley*, the court affirmed the position that privilege can apply in the context of a regulatory investigation where expert input is sought and provided. In that case, the respondent resisted access to documents on the basis that they were legally privileged ‘for the purpose of providing instructions and obtaining legal advice and also in contemplation or furtherance of litigation and an investigation’ by the ODCE. The court accepted the respondent’s argument that electronic communications between a company director, his solicitor and an IT employee attaching a draft response to a request from the ODCE during the course of a statutory investigation were protected by privilege where the communication was issued ‘for the purposes of advancing the respondent’s draft statement and was sent on a confidential basis and without a waiver of privilege by the respondent’.

In *Kurtz v. Dunnes Stores*, the court confirmed that privilege could be claimed over witness statements and internal investigation forms on the basis that they were made in anticipation of litigation. In that case, the plaintiff suffered injuries following a fall in the respondent’s store. The respondent made discovery of certain documents relating to the incident but claimed privilege over witness statements and internal investigation forms on the basis that these were made in anticipation of litigation. The court applied the test from *Artisan Glass Studio Ltd v. The Liffey Trust Ltd*, finding that litigation was reasonably apprehended at the time the documents in question were brought into being and the documents in question

---

17 [2019] IEHC 44.
18 [2018] IEHC 278.

© 2020 Law Business Research Ltd
were brought into being for the purpose of that litigation. As there was nothing to suggest to the court that the documents were created for any other purpose, and as the respondent discharged the onus to show the documents were covered by privilege, the application was refused.

Privilege over any document is a right of the client, which he or she may choose to waive. In general, the disclosure of an otherwise privileged document to a third party will waive privilege. However, following the decision in *Fyffes v. DCC*,\(^{19}\) the courts will permit the disclosure of an otherwise privileged document to a third party for a limited and specified purpose without privilege being waived. In these circumstances, it is essential that the entity making the disclosure seeks assurances by way of a confidentiality agreement that the recipient will not disclose the privileged documents and will use them only for the specified and limited purpose for which they have been disclosed. The UK courts have found in *Sports Direct International plc v. Financial Reporting Council*\(^{20}\) that the protection extends to privileged documents in the context of an investigation into an auditor concerning an audit. Both the client (therein *Sports Direct International plc*) and the auditor can exercise this privilege, while previously it was only applicable where the client was subject to a request for disclosure.

Therefore, in the context of regulatory investigations, legal professional privilege is relevant when considering the power of regulatory authorities to inspect documentation and compel the production of documents.

### iii Whistle-blowers

The Protected Disclosures Act 2014 (the Protected Disclosures Act) is the key piece of legislation in relation to reporting suspicions of illegal activity. It is the first comprehensive piece of legislation governing whistle-blowing, where previously only piecemeal provisions existed. Public sector bodies must now put in place whistle-blowing policies that meet the requirements of the Protected Disclosures Act; and where private sector companies have policies in place, they must review them to ensure they are aligned to the provisions of the Protected Disclosures Act. The Industrial Relations Act 1990 (Code of Practice on Protected Disclosures Act 2014) (Declaration) Order 2015 (the Code of Practice) gives guidance on what should be contained in a whistle-blowing policy.

Part 3 of the Protected Disclosures Act sets out the protections offered to those who make protected disclosures. If a worker makes a protected disclosure, the employer in question may face liability for dismissing or penalising the worker, bringing an action for damages or an action arising under criminal law, or disclosing any information that might identify the person who made the disclosure. Further, the Protected Disclosures Act makes provision for a cause of action in tort for the worker for detriment suffered as a result of making a protected disclosure.

Section 5 of the Protected Disclosures Act as amended defines a ‘protected disclosure’ as a disclosure of relevant information, made by a worker, which, in his or her reasonable belief, shows a ‘relevant wrongdoing’ and which came to his or her attention in the course of his or her employment. Section 5(3) of the Protected Disclosures Act defines a ‘relevant wrongdoing’ as:

\[\text{a} \quad \text{relating to the commission of an offence;}\]

---

20 [2020] EWCA Civ 177 (Rose LJ).
b non-compliance with a legal obligation (except one arising under the worker’s employment contract);
c a miscarriage of justice;
d endangerment of health and safety;
e damage to the environment;
f misuse of public funds;
g mismanagement by a public body; or
h concealing or destroying information relating to any of the above.

The definition of ‘worker’ in Section 3 of the Protected Disclosures Act is also quite broad in its scope and covers employees (including temporary and former employees), interns, trainees, contractors, agency staff and consultants.

The Protected Disclosures Act also sets out a procedure for redress for a worker who makes a protected disclosure. If the matter is part of an unfair dismissals claim by the worker and an Adjudication Officer of the Workplace Relations Commission finds in favour of the worker, it can require the employer to take a specified course of action or require the employer to pay compensation of up to 260 weeks’ remuneration to the worker.\(^2^1\)

Save in respect of disclosures that involve the disclosure of trade secrets (see below), the motivation for making a disclosure is irrelevant and there is no obligation that such a disclosure must be made in the public interest. This provision aims to protect companies from malicious and ill-founded claims.

The Protected Disclosures Act closely reflects, and brings Ireland in line with, international best practice in the area. In achieving its principal aim of protecting those who make a protected disclosure from reprisal from their employers, it places a significant burden on employers in all sectors to ensure they have adequate policies in place and conform to their requirements.

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (the Whistleblower Directive) came into force on 23 October 2019. The standards proposed largely reflect those in place in Ireland already, but the most likely impact would be the potential broadening of the definition of what is a protected disclosure. Member States have until 17 December 2021 to ensure that domestic law complies with the directive.

In addition, a new EU-wide directive concerning trade secrets (Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (the Trade Secrets Directive)) was given legal effect in Ireland in June 2018 by way of the European Union (Protection of Trade Secrets) Regulations 2018. The 2018 Regulations provide for civil redress measures and remedies if a trade secret is unlawfully acquired, used or disclosed, and stipulate that a whistle-blower must prove their motivation for revealing trade secrets as part of the protected disclosure where they decide to so. Before this amendment, the motivation of a whistle-blower was not relevant. Pursuant to the 2018 Regulations, whistle-blowers may be liable to a fine of €50,000 and a three-year custodial sentence for making a protected disclosure, using trade secrets, where the individual cannot prove that the disclosure was motivated by the protection of the general public interest.

\(^2^1\) Sections 11 and 12 of the Protected Disclosures Act 2014.
III ENFORCEMENT

i Corporate liability

The Interpretation Act 2005 provides that in all Irish legislation, any reference to ‘persons’ includes references to companies and corporate entities. Therefore, a company can, in theory, be subject to criminal or civil liability in the same manner as an individual and can be liable for the conduct of its employees and officers. However, corporate liability has predominantly been restricted to offences where a fault element (mens rea) is not required, namely those of absolute, strict and vicarious liability. Many regulatory offences carrying corporate liability are established as such offences.

For example, Section 343(11) of the Companies Act 2014 imposes absolute liability in circumstances where a company fails to send its annual financial accounts to the Company Registrations Office and provides that the company will be guilty of an offence. In contrast, Section 271 of the Companies Act 2014 provides that an officer of a company will be presumed to have permitted a default by the company, unless the officer can establish that he or she took all reasonable steps to prevent the default, or was unable to do so by reason of circumstances beyond his or her control. Under the recently enacted Criminal Justice (Corruption Offences Act) 2018 (the Corruption Offences Act), a company can be held liable for corrupt actions committed for its benefit by any director, manager, secretary, employee, agent or subsidiary, unless the company can demonstrate that it took ‘all reasonable steps and exercised all due diligence’ to avoid the offence being committed.

Additionally, the Competition Act 2002 imposes vicarious liability by providing, for the purposes of determining the liability of a company for anticompetitive practices or abuse of a dominant position, that the acts of an officer or employee of a company carried out for the purposes of, or in connection with, the business affairs of the company will be regarded as an act of the company.

While theoretically a company can be guilty of a mens rea offence, the means of attributing the acts of an employee to a company for the purposes of criminal liability is not settled in Irish law. The Irish and English courts have recognised two modes of importing direct liability to a company: the identification doctrine and the attribution doctrine. The former focuses on the extent to which the individual employee or officer who committed the offence represents the ‘directing mind and will’ of the company, thereby rendering the company criminally liable. The attribution doctrine, on the other hand, is not concerned with the individual’s position in the company, but rather imposes a form of absolute liability on companies where their officers or employees commit offences in the course of, and connected with, their employment. While there is conflicting jurisprudence on the preferred approach, only the identification doctrine has been endorsed by the Irish Supreme Court, albeit in the context of the imposition of civil liability on a corporation. The uncertainty in this area about the correct test to apply to determine to criminal liability of a corporate has led the Law Reform Commission to make a number of recommendations for reform in this area in its 2018 Report on Regulatory Powers and Corporate Offences.

If it is proposed that companies and individuals would be represented by the same counsel, the rules governing conflicts of interest in the Solicitors’ Code of Conduct would warrant consideration, which provides that: ‘if a solicitor, acting with ordinary care, would

II Penalties

Irish criminal legislation typically provides for monetary fines or terms of imprisonment for offences. Given the nature of corporate entities, the most common form of sanction against a corporate entity is a fine. However, while less common, legislation also provides for compensation orders (whereby the guilty party is required to pay compensation in respect of any personal injury or loss to any person resulting from the offence), adverse publicity orders (in the form of publication of the offence and the identity of the entity found guilty) and remedial orders (to undo the harm caused by the offence).

Another common sanction against directors of companies is a disqualification order. Under Section 839 of the Companies Act 2014, where a person has been convicted of an indictable offence in relation to a company, or convicted of an offence involving fraud or dishonesty, that person may not be appointed to, or act as, an auditor, director or other officer, receiver, liquidator or examiner or be in any way, whether directly or indirectly, concerned or take part in the promotion, formation or management of any company.

The CBI also operates the Administrative Sanctions Procedure pursuant to the Central Bank Act 1942, as amended. This legislation bestows a range of sanctions at the CBI’s disposal. Part IIIC, as amended, sets out the powers of the CBI to impose sanctions in respect of the commission of prescribed contraventions by regulated financial services providers. The monetary penalty for financial institutions is an amount up to €10 million or 10 per cent of the annual turnover of the regulated financial service provider in the last financial year, whichever is the greater. As mentioned above, since 2006, the Central Bank has imposed 134 fines on regulated entities under its Administrative Sanctions Procedure, bringing total fines imposed by the Central Bank to over €103 million. The CBI has used these powers to reach settlements with financial institutions for regulatory breaches. In addition, the CBI has the power to suspend or revoke a regulated entity’s authorisation in respect of one or more of its activities. The Law Reform Commission has recommended in its 2018 Report on Regulatory Powers and Corporate Offences that the Administrative Sanctions Procedure should, subject to some reforms, be extended to similarly situated financial and economic regulators.

A wide range of penalties exist under the Competition (Amendment) Act 2012. The maximum prison sentence for an offence relating to anticompetitive agreements, decisions and concerted practices is 10 years, and the maximum monetary penalty is a fine of €5 million.

---

23 Section 6(1) of the Criminal Justice Act 1993 as amended.
25 Sections 75 and 85 of the Consumer Protection Act 2007, as amended by the European Union (Consumer Information, Cancellation and Other Rights) Regulations 2013; Section 1078(3A) of the Taxes Consolidation Act 1997.
26 The Central Bank (Supervision and Enforcement) Act 2013.

© 2020 Law Business Research Ltd
or 10 per cent of turnover. Further, the Irish courts have jurisdiction under the Companies Act 2014 to disqualify an individual from acting as a director of a company if that individual is convicted of a competition offence on indictment.

Under the Corruption Offences Act, if convicted, a company or an individual is liable to a fine of up to €5,000 on summary conviction or an unlimited fine on conviction on indictment. On conviction, an individual may also be liable to up to 12 months’ imprisonment on summary conviction and up to 10 years’ imprisonment on indictment, together with the forfeiture of any gift, consideration or advantage obtained in connection with the offence or property to the value of such gift, consideration or advantage. With regard to a public official, a court may order that they be removed from their public position. The court can also prohibit those convicted of corruption offences from seeking public appointment for up to 10 years.

iii Compliance programmes

Compliance programmes are not generally provided for in legislation as a defence to criminal proceedings. The Corruption Offences Act was commenced on 30 July 2018 and is the principal statutory source of bribery law in Ireland repealing the Public Bodies Corrupt Practices Act 1889 and the Prevention of Corruption Act 1906–2010. The Corruption Offences Act has consolidated and modernised the Irish law in this area and is expected to have a significant impact on corporates operating in Ireland. A notable provision, similar to the content of Section 7 of the UK Bribery Act 2010, is Section 18(2) of the Corruption Offences Act, which provides that a company may be held liable for the corrupt actions committed for its benefit by any director, manager, secretary, employee, agent or subsidiary. The Corruption Offences Act contains an explicit defence for a company charged with an offence under Section 18 if it can show that the company took ‘all reasonable steps and exercised all due diligence to avoid the commission of the offence’.

If a company is found guilty of an offence, a wide range of factors may be taken into account when sentencing and these are at the discretion of the court. Mitigating factors include whether the company ceased committing the criminal offence upon detection or whether there were further infringements or complaints after the offence was detected, whether remedial efforts to repair the damage caused were used by the company and whether the company itself reported the infringement before it was detected by the prosecuting authority. Additionally, in imposing any sentence, the court must comply with the principle of proportionality as set out in People (DPP) v. McCormack. The existence and implementation of a compliance programme may assist in reducing the quantum of any sentence to be imposed, but there is no legislative mechanism for this.

27 Section 2 of the Competition (Amendment) Act 2012.
28 Section 839 of the Companies Act 2014.
29 Section 17(1)(a) of the Criminal Justice (Corruption Offences) Act 2018.
30 id., Section 17(1)(b).
31 id., Section 17(4)(b).
32 id., Section 17(4)(c).
iv Prosecution of individuals

When there are allegations of an individual’s misconduct in the course of his or her employment, the company may first conduct an internal investigation into the alleged offence. If the company concludes that the alleged conduct did take place, the company may be required to report this activity to the relevant authorities. During this investigation, the individual may be placed on ‘gardening leave’ or be suspended. However, in the case of Bank of Ireland v. O’Reilly, the High Court stipulated that employers must exercise extreme care when suspending an employee pending an investigation.34

However, if criminal prosecution precedes an internal investigation, in general, internal disciplinary procedures are suspended, based on respecting the individual’s right to silence. Notably, the High Court has decided that the acquittal of an employee of criminal charges does not preclude employers from considering whether an employee should or should not be dismissed on the basis of the impugned conduct.35

There is a prohibition on indemnifying directions in respect of any liability that would otherwise attach to him or her in respect of any negligence, default, breach of duty or breach of trust of which he or she may be guilty in relation to the company.36 However, the Companies Act 2014 also provides that a company may purchase and maintain, for any of its officers or auditors, directors and officers (D&O) insurance in respect of any liability arising under negligence, default, breach of duty or breach of trust.37 Accordingly, a company may indemnify an officer of the company for any liability incurred by him or her in defending the proceedings, whether civil or criminal, provided judgment is given in the individual’s favour or the individual is acquitted.38 In practice, D&O policies tend to exclude losses resulting from fraud or dishonesty, malicious conduct and the obtaining of illegal profit.

The Corruption Offences Act provides for the criminal liability of corporate bodies where a director, manager, secretary or other officer, employee or subsidiary commits an offence with the intention of obtaining or retaining business or an advantage in the conduct of business.

Almost all modern Irish regulatory legislation includes a standard provision allowing the imposition of personal criminal liability on directors, managers or other officers of a company, if the company commits an offence. Typically, this standard provision states:

Where an offence under this Act is committed by a body corporate or by a person acting on behalf of a body corporate and is proved to have been so committed with the consent, connivance or approval of, or to have been facilitated by any neglect on the part of any director, manager, secretary or any other officer of such body, such person shall also be guilty of an offence.

The Corruption Offences Act also provides under Section 18(3) that, where a corruption offence was committed with the consent, connivance, or was attributable to the wilful neglect, of a person who was a director, manager, secretary or other officer of the body corporate, or a person purporting to act in that capacity, then the individual may also be found liable in their personal capacity.

36 Section 235 of the Companies Act 2014.
37 Section 235(4) of the Companies Act 2014.
38 id., Section 235.
Although, to date, prosecutions of individuals under such provisions are relatively rare, it is worth mentioning a recent decision of the Court of Appeal, *DPP v. TN*\(^3\) where the court found a manager may be prosecuted for company offences where he or she has functional responsibility for a significant part of the company’s activities and has direct responsibility for the area in controversy. The court observed that, in the modern business environment, responsibilities are distributed such that it is difficult to say that one individual is responsible for the management of the whole of the affairs of a company. A ‘manager’ does not have to be actively involved in every area of the company’s business. The individual in this case, Mr TN, had no involvement in the financial side of the business, but he had direct responsibility for the operation of the facility and for compliance with the terms of its waste licence.

### IV INTERNATIONAL

#### i Extraterritorial jurisdiction

Ireland does not, in general, assert extraterritorial jurisdiction in respect of acts conducted outside the jurisdiction. However, extraterritorial jurisdiction may be conferred by statute to varying degrees. For instance, Section 4 of the Competition Act 2002 provides that it is an offence to be a party to an anticompetitive agreement that has the effect of preventing, restricting or distorting competition in trade in goods or services within the state. Importantly, the Section is not restricted to agreements made within Ireland.

There are a number of specific offences for which Ireland exercises extraterritorial jurisdiction.

**Corruption**

As mentioned, the Corruption Offences Act was introduced on 30 July 2018. The Corruption Offences Act is designed to consolidate a range of legislation enacted between 1889 and 2010 and introduce new offences and other revisions, some of which derive from the Tribunal of Inquiry into Certain Planning Matters and Payments. The Act further modernises anti-corruption laws and will help Ireland meet its commitment to various international anti-corruption instruments, such as EU Council Decisions, the United Nations Convention on Corruption, the OECD Convention on Bribery of Foreign Public Officials and the Council of Europe Criminal Law Convention on Corruption.

**Money laundering**

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the CJ(MLTF) Act) sets out specific circumstances in which an action can be interpreted as money laundering outside Ireland. If an individual or a company engages in conduct in a foreign jurisdiction that would constitute a money laundering offence both under the CJ(MLTF) Act and in that foreign jurisdiction, they can be prosecuted in Ireland. This extraterritorial jurisdiction may only be exercised if the individual is an Irish citizen, ordinarily resident in the state; or the body corporate is established by the state or registered under the Companies Act.

The Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018 came into force on 26 November 2018. This act gives effect to the EU Fourth

---

39 *DPP v. TN* [2018] IECA 52.

40 Section 8 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.
Money Laundering Directive (Directive 2015/849 (4AMLD)) and makes a range of amendments to existing anti-money laundering (AML) legislation set out in the Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010 and 2013. The Act itself imposes increased responsibility on ‘obliged entities’ to identify and assess potential risks of money laundering and terrorist financing in their business relationships and transactions. Aside from the requirement to identify individuals holding ultimate beneficial ownership, the most important change it introduces in Irish law is the inclusion of both domestic and foreign politically exposed persons (PEPs) under the new rules. Previously, only foreign PEPs were subject to a mandatory enhanced regime.

The Fifth Anti-Money Laundering Directive (5AMLD) was implemented into Irish law by way of the European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019. These regulations provided for the creation of the New Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies, which came into operation on 22 June 2019. On 17 May 2019, Ms Seana Cunningham, Director of Enforcement and Anti-Money Laundering at the Central Bank, in a speech delivered at the Professional, Regulatory & Disciplinary Bar Association’s Annual Conference, emphasised that the regulatory focus on AML at a national and EU level will continue.

ii International cooperation

The Criminal Justice (Mutual Assistance) Act 2008 (the Mutual Assistance Act) is the primary piece of legislation governing mutual legal assistance between Ireland and other countries. The extent of available cooperation under mutual legal assistance procedures is dependent on the identity of the corresponding state. The greatest level of cooperation exists between Ireland and other EU Member States. Cooperation with third countries (those outside the European Economic Area) is dependent on their ratification of relevant international agreements or the existence of a mutual assistance treaty agreed between them.

Most notably, the Mutual Assistance Act allows Ireland to take evidence in connection with criminal investigations or proceedings in another country, search for and seize material on behalf of another country, serve a summons or any other court process on a person in Ireland to appear as a defendant or witness in another country, and transfer a person imprisoned in Ireland to another country to give evidence in the foreign criminal proceedings.

In April 2018, the European Commission proposed a legislative package, which actually consists of two strongly interconnected proposals:

a a Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters; and

b a Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, which is often referred to as the proposal on ‘E-evidence’.

The E-evidence proposal will make it faster and easier for law enforcement authorities of Member States to obtain cross-border evidence. E-evidence proposes to introduce European Production and Preservation Orders in criminal matters. In effect, it allows a competent authority from one Member State to make a direct request to service providers in other Member States to obtain access to, or preservation of, electronic data for criminal investigations.

---

41 SI No. 110/2019.
42 As amended by the Criminal Justice (Mutual Assistance) (Amendment) Act 2015.
There are a number of additional measures in place to facilitate Ireland’s cooperation with other EU Member States, including the Council Framework Decision on Freezing Orders and the Council Framework Decision on the European Evidence Warrant. In addition to this, Council Regulation 1206/2001\(^{43}\) allows a court in another EU Member State (other than Denmark) to take evidence from a witness connected to court proceedings in Ireland. This is provided for under the Rules of the Superior Courts.\(^{44}\)

Ireland is subject to the European Arrest Warrant Framework Decision, which was implemented by virtue of the European Arrest Warrant Act 2003, as amended by the European Arrest Warrant (Application to Third Countries and Amendment) and Extradition (Amendment) Act 2012. This governs all extradition procedures between EU Member States. The High Court is the competent authority for issuing a European arrest warrant if the individual sought is accused of an offence for which the maximum penalty is at least one year in prison, or if he or she has already been sentenced to a prison term of at least four months. A European arrest warrant does not have a dual criminality requirement – meaning the offence must be prohibited under the domestic law of both countries – for certain serious offences, such as corruption, fraud or money laundering. This legislation can extend to individuals from non-EU countries upon consultation between the Minister for Foreign Affairs and the Minister for Justice and Equality. Generally, extradition to non-EU countries is governed by the Extradition Act 1965, as amended (the Extradition Act). There are a number of preconditions to non-EU extradition. First, there must be an extradition agreement in place between Ireland and the non-EU country before an extradition can take place. Second, the Extradition Act retains a requirement of dual criminality. Third, the Extradition Act excludes extradition for political, military and revenue offences.

While there is currently a lot of uncertainty concerning what a post-Brexit United Kingdom will look like, it is likely that in a no-deal scenario, the United Kingdom will no longer be party to Europol or Eurojust, and no longer operate the European Arrest Warrant. Instead, according to the Law Enforcement and Security (Amendment) (EU exit) Regulations 2019, it will revert to the 1957 European Convention on Extradition regime. The Irish Government’s General Scheme of the Miscellaneous Provisions (Withdrawal of the United Kingdom from the European Union on 29 March 2019) Bill 2019 likewise proposes application of the European Convention on Extradition regime to extradition between the United Kingdom and Ireland. This may have a negative impact on the efficiency with which the United Kingdom will be able to combat illicit activity after Brexit occurs. The UK Serious Fraud Office has also indicated that loss of access to EU measures and tools in this context will adversely affect investigations and prosecutions, representing a strategic risk to the United Kingdom.

The transposition of the EU 4AMLD into Irish law has also led to further enhanced international cooperation, as the Directive requires information to be shared between competent national authorities, including the creation of a central register of beneficial owners of entities. Under the 5AMLD commencing on 22 July 2019, the Register of Beneficial Ownership has effectively broadened the inspection net to the public in most cases. The

\(^{43}\) Council Regulation (EC) No. 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

\(^{44}\) Order 39 Rule 5 Rules of the Superior Courts.
The initial filing deadline to provide details of beneficial ownership was 22 November 2019. The regulations require all newly incorporated companies and Industrial and Provident Societies to register their beneficial ownership details within five months of incorporation.

The European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019 came into force on 22 March 2019, save for Part 3. Part 3 concerns the new Central Register of Beneficial Ownership, which became operative on 22 June 2019. The aim of the 2019 Regulations is to bring Ireland’s beneficial ownership regulations in line with the 4AMLD as amended by the Fifth Money Laundering Directive. Therefore, the 2019 Regulations established the New Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies (Register) on 22 June 2019. Companies have five months from date of incorporation to provide details of their ownership to the Register.45

### iii Local law considerations

There are a number of legal considerations to be aware of in relation to a cross-jurisdictional investigation, in particular in the areas of banking confidentiality, data privacy and constitutional law.

An obligation of bank–client confidentiality is implied by common law. However, this obligation can be breached in limited circumstances, including where the terms of the contract with the customer so provide or a bank is compelled by law to disclose information.46

The GDPR became effective across the EU Member States on 25 May 2018. The GDPR introduces significant changes to data subject rights, supervision and enforcement, and the scope of the application of EU data protection law in that companies based outside the EU will be subject to GDPR when offering services in the EU. The Law Enforcement Data Protection Directive 2016 (the 2016 Directive)47 was adopted in parallel with GDPR and governs the processing of personal data by data controllers for ‘law enforcement purposes’, which falls outside the scope of the GDPR. The Data Protection Act 2018 gives further effect to the GDPR and the 2016 Directive while largely, though not entirely, repealing the previous Data Protection Acts. The Data Protection Act 2018 was signed into law on 24 May 2018, to coincide with the coming into effect of the GDPR.

Litigation surrounding data subject rights took place throughout 2019. On 19 December 2019, the Advocate General of the Court of Justice of the EU delivered his opinion in Facebook Ireland and Schrems48 regarding the use of standard contractual clauses to transfer data to non-EU member countries. The opinion, while not binding on the Court, shifts the burden to the Data Protection Commissioner to assess whether such countries have sufficient safeguards to protect EU data subjects’ rights.

The Irish High Court considered whether CCTV footage collected for security purposes could be used in a disciplinary investigation. It found in Doolin v. Data Protection Commissioner49 that the data retained for security purposes could not subsequently be processed for the purposes of disciplinary hearings without having lawful grounds to do so under GDPR.

46 Tournier v. National Provincial and Union Bank (1924) 1 KB 461.
48 Facebook Ireland and Schrems Case C-311/18.
49 [2020] IEHC 90.
Further, Irish individuals or entities who are the subject of an international investigation benefit from the protection of the Irish Constitution and the European Convention on Human Rights, including the right to a good name and the right to a fair trial.

V YEAR IN REVIEW

During 2019, the government made significant progress in implementing the proposals set out in the Measures to Enhance Ireland’s Corporate, Economic and Regulatory Framework. This included further review of the proposals for the General Scheme of the Companies (Corporate Enforcement Authority) Bill 2018. Under this Bill, it is proposed that the ODCE will be re-established as an agency, in the form of a commission, which will be known as the CEA. The new agency will have more autonomy and flexibility to adapt to the challenges it faces in encouraging greater compliance with the Companies Act. The Bill is currently before the Oireachtas in the committee review phase. In addition, in 2018, the Minister for Justice and Equality appointed former DPP Mr James Hamilton to chair a review of Ireland’s anti-corruption and anti-fraud structures and procedures in criminal law enforcement. This review will assess the extent to which the various state bodies involved in the prevention, detection, investigation and prosecution of fraud and corruption are working effectively together, and to identify any gaps and impediments in this regard. The review underwent a public consultation on 13 March 2019, which concluded on 19 April 2019.

The ODCE and the Central Bank have also been vocal about their commitment to advancements in their investigative practices and procedures. The ODCE reported key hires including forensic accountants, a digital forensic specialist, enforcement lawyers and enforcement portfolio managers. The OCDE has also reported advancements in relation to their forensic capabilities, such as the establishment of an in-house digital forensics laboratory, including an on-site digital forensics capability whereby data retrieved from digital devices can be relayed to investigators in real time. The Director has continued to progress its investigation into Independent News and Media, with the High Court receiving the first report into the conduct of affairs within the company on 11 April 2019. An investigation into the Football Association of Ireland commenced in 2018 subsequent to its auditors filing a notice to the Companies Registration Office alleging breaches of the Companies Acts on the grounds that financial accounts were not properly maintained. This investigation continued throughout 2019 and is ongoing in 2020.

The renewed focus on measures to enhance Ireland’s approach to corporate misconduct is both timely and significant given the uncertainty surrounding Brexit. However, the Political Declaration published on 22 November 2018 emphasises the commitment to mutual cooperation, stating that reciprocal equivalence frameworks will be put in place enabling both the European Union and the United Kingdom to declare a third country’s regulatory and supervisory regimes ‘equivalent’. The most recent round of EU–UK Future Relationship Negotiations took place between 11 and 15 May 2020, with the issue of regulatory equivalence reportedly remaining a difficult point to resolve between negotiators.
VI CONCLUSIONS AND OUTLOOK

Ireland has a robust regime for the investigation and prosecution of corporate misconduct that helps to maintain its reputation as a low-risk country in which to do business. The government has signalled its intention in recent years to ensure that the legal and regulatory environment continues to be subject to regular scrutiny and review so that it is strengthened appropriately to meet emerging risks and challenges. With that in mind, it seems likely that we will continue to see more enforcement across all regulated sectors in the future.

53 Measure to enhance Ireland’s Corporate, Economic and Regulatory Framework.
I INTRODUCTION

Corporate misconduct in Italy is punishable under both criminal and administrative law. The public prosecutor directs preliminary investigations in criminal prosecutions and issues orders to the police, who investigate.

Under the terms of the Constitution, the Public Prosecutor’s Office is independent of all political influence.

The Office theoretically has no discretion as to which offences must be prosecuted: under the mandatory prosecution principle (Article 112 of the Constitution), the public prosecutor must always issue a request for indictment (a request to submit the defendant to trial) if, at the end of the investigation, he or she has found sufficient evidence that a crime has been committed. In practice, the rule is disregarded: the high number of reports of criminal offences imposes a de facto selection of the cases to be dealt with by the investigating authorities, depending on the circumstances, in accordance with the principle of priority.

Some kind of jurisdictional control on the decision of the prosecutor as to which cases to dismiss, and which to prosecute, is in any case granted by the judge of the preliminary investigations, who has the final word on any request for dismissal.

When the prosecutor investigates the possible criminal liability of corporate entities, under Legislative Decree No. 231 of 8 June 2001 (Decree 231/2001) (see Section III), the mandatory prosecution principle may be bypassed, because in this case there is no jurisdictional control over the prosecutor’s dismissal decision; only the prosecutor’s hierarchical superior may personally take any further appropriate action.

From an administrative perspective, the independent administrative authorities have specific powers relating to their individual remits. If the officials of any of the authorities discover any offences in the course of their duties, these bodies are obliged to report them to the judicial authorities.

Far-reaching powers are granted to the Italian Securities and Exchange Commission (CONSOB) under the Consolidated Law on Finance, with reference to insider trading and market-manipulation offences, and in close cooperation with the public prosecutor. Further, the latter is under an obligation to notify the president of CONSOB when a report of a

---

1 Mario Zanchetti is a founding partner of Studio Legale Pulitano-Zanchetti.
2 The most important of these for companies include the Bank of Italy, the Italian Securities and Exchange Commission (CONSOB), the Italian Insurance Supervisory Authority (the Italian insurance regulator since 1 January 2013, replacing the former authority, ISVAP), the Italian Competition Authority (Antitrust) and the Italian Data Protection Authority.
3 Legislative Decree No. 58 of 24 February 1998.
criminal offence of which he or she has been made aware involves insider trading or market manipulation by listed companies, with a view to obtaining a reasoned technical opinion on the matter from this independent authority. The main powers granted to CONSOB include the right to:

a. request documents from any party that may have relevant information;
b. interview individuals in person;
c. carry out inspections; and

d. gain direct access to data contained in the Italian Central Credit Register at the Bank of Italy.

At the end of its own investigation, CONSOB may issue severe administrative sanctions for the offences of market abuse (insider trading, market manipulation), which are meant to be added to the criminal punishment (up to 12 years’ imprisonment), for the same facts. In a breakthrough decision, the European Court of Human Rights has convicted Italy, considering this doubling of penalties for the same offences as contrary to the *ne bis in idem* principle, provided for in the European Convention on Human Rights, Section 6.\(^4\) Italy will probably have to rethink the entire system of ‘double track’ persecution of corporate offences, both in criminal courts and before the administrative authorities, which has been very typical up to now (not only for financial crimes but also for tax crimes and many others).

Besides the foregoing, an increasingly important role has been attributed to the National Anti-Corruption Authority (ANAC), which has the general function of preventing corruption in public offices and now also supervises the conclusion and execution of public contracts. ANAC may also issue sanctions (disqualifications, etc.).

As regards the issue of cooperation between the company under investigation (or its employees) and the investigating body, the presumption of innocence and the right to due process of law (both of which are constitutional principles) categorically exclude any legal obligation to cooperate. However, for an appropriate choice to be made regarding cooperation, a case-by-case assessment must be made of:

a. the nature of the case;
b. the seriousness of the alleged conduct;
c. any incriminating evidence;
d. the identity and investigative approach of the public prosecutor; and
e. the possible repercussions of failure to cooperate with the investigating bodies (e.g., the risk of being subject to pretrial precautionary measures).

The decision as to whether and how to cooperate typically remains part of any defence strategy, both for the individual defendant and for the corporation. In practice, the burden of the interdictory sanctions that may hit the corporation, in cases in which Decree 231/2001 may be applied (see Section III) weakens the presumption of innocence and makes cooperation almost a default option for the corporation; considering also that, under a typical ‘carrot and stick approach’, Decree 231/2001 provides certain incentives, such as the reduction of fines and the preclusion of bans, to corporations that cooperate and bargain a plea.

In such cases, prior to the initiation of trial proceedings, companies must:

a. make good any damages in full;

\(^4\) *Grande Stevens and Others v. Italy*, 4 March 2014.
b eliminate the harmful and dangerous consequences of the offence (or otherwise take action to this effect);
c adopt and implement organisational models capable of preventing offences of the type that were committed or eliminate the organisational shortcomings that led to the offences; and
d hand over any profits earned for confiscation.

Therefore, if a corporation is directly involved in the proceedings, a cooperative strategy must always be carefully considered.

II CONDUCT

i Self-reporting
As a matter of principle, under Italian law, private individuals and businesses have the right – but not the obligation – to report to the judicial authorities any offences that may come to their attention. With the exception of some specific cases, the decision whether to report an offence is exclusively down to each individual's sense of civic duty, and there is no provision for any benefit or incentive.

ii Internal investigations
Italian law allows investigations to be carried out by a lawyer appointed as defence counsel in a criminal proceeding by a person or a corporation, or before any proceedings are initiated. Any evidence collected in this way may be used in any subsequent criminal proceedings. Italian law allows the lawyer to carry out both ordinary and extraordinary inquiries. Information is collected by the lawyer from persons with relevant information; they do not need to be accompanied by lawyers, but they are under an obligation to tell the truth, the violation of which is punished by the Criminal Code. The situation is different if the person to be questioned is a suspect in the proceedings, in related proceedings or for a related offence; in these cases, the presence of a lawyer is mandatory. The case is also different if the witness may be called upon to make self-incriminating statements, in turn risking becoming a suspect; in such cases, the questioner must stop the interview immediately.

Some witnesses with specific qualifications also have the right in criminal proceedings not to answer questions when the answer would entail a violation of professional privilege. This right is granted only to professionals expressly mentioned in the Code of Criminal Procedure or under special legislation, such as lawyers.

Lawyers receive absolute protection at all stages and instances of proceedings, both with reference to attorney–client communications and to work product. It should be borne in mind, however, that under Italian case law, in-house counsel may not be granted the same privileges as external lawyers, and their computers, emails and hard copies of documents may be subject to search by investigating authorities.

5 For example, in cases involving the receipt of property resulting from the commission of a criminal offence, the notification of the planting of explosives at the company's location or the theft of weapons or explosives, businesses are obliged to self-report.
6 There is no obligation of disclosure; therefore, the investigating lawyer may well decide not to submit to authorities any evidence collected.
Finally, investigations may be done internally by the staff of the establishment or by independent external advisers. In the first case, investigations are typically carried out by the internal audit service with the backing of the legal department. The advantages of this type of investigation are in terms of lower costs and greater knowledge of the company; however, this type of investigation might not be capable of providing a high enough level of expertise and independence. The internal independent investigation is entrusted instead to independent external advisers that support the administrative and supervisory bodies. The external advisers certainly guarantee better expertise and independence.

iii Whistle-blowers

There was no general provision in Italy regarding whistle-blowing until 30 November 2017, when Law No. 179 concerning whistle-blowing entered into force.

The text regulating whistle-blowing has gradually emerged as part of the debate in recent years between European and international institutions on the need to introduce valid measures to fight corruption.

The first important Italian intervention in this sense took place with the approval of the Law No. 190, which entered into force on 27 November 2012 (the Severino Law), limited to public administration, which introduced specific provisions concerning the protection of public servants who report abuse. This discipline, however, did not find application in the private sector and required certain additions and revisions to align with the simultaneous evolution of public employment regulations.

The revised regulation of 2012 replaced Article 54-bis of Legislative Decree No. 165, of 30 March 2001, providing for the protection of the public employee who, in the interests of public administration, reports violations or unlawful conduct of which he or she became aware on the basis of his or her employment relationship. The employee cannot be subjected to retaliation because of the report (including sanctions, dismissal, demotion or transfer to other offices) or be subjected to any other measures that might have a negative effect on his or her working conditions.

These reports may be sent either to the internal manager of the corporate structure responsible for preventing corruption and transparency, or to the ANAC, or directly to the ordinary or accounting judicial authority depending on the nature of the report.

Among the peculiarities of the new discipline is confirmation of the prohibition to reveal the identity of the whistle-blower, whose name must be protected:

- in the event of a criminal trial, in the manner and timing established by Article 329 of the Criminal Code;
- in the event of an accounting process, from the prohibition to reveal his or her identity until the end of the preliminary phase; and
- in the event of an administrative process, from the prohibition of disclosing his or her identity without his or her consent.

The ANAC is the authority responsible for applying administrative sanctions.

Specifically, the ANAC can apply a penalty of between €5,000 and €30,000, charged to those responsible for retaliatory measures against the reporting agent. A significantly higher penalty, of between €10,000 and €50,000, is envisaged if the absence of an internal system for reporting violations is ascertained or if it is found that the system manager has not verified or analysed the reports received as part of their activity.
Any discrimination or retaliation against the reporter must in any case be justified by the public administration, which bears the burden of proving and justifying that such measures have been taken for reasons unrelated to the notification.

If it is proved that the employee has been dismissed for reasons related to an alert, that employee has the right to be reinstated in the workplace, to compensation for damage and payment of social security contributions due for the period between dismissal and reinstatement.

The risk of a distorted use of the whistle-blowing instrument has been mitigated with the cancellation of any protection if the reporting person is convicted, even at first instance, in criminal proceedings for slander, defamation or other similar crimes committed through the reporting, or, is subject to civil liability if fraud or gross negligence is established.

In addition to introducing significant changes regarding the protection of the public employee who reports an offence, the law provided some modifications to Decree 231/2001 (see Section III) with regard to the protection of employees or collaborators who report illegal activities in the private sector.

Law No. 179/2017, adding three new paragraphs to Article 6 of Decree 231/2001, requires that a model of organisation and governance (MOG) adopted by a company provides for:

- adequate information channels that, ensuring the confidentiality of the identity of the reporting agent, allow individuals in senior positions and those subordinated to them to submit detailed reports of illicit conduct or of violations of the MOG;
- at least one alternative signal channel that guarantees the privacy of the reporters;
- the prohibition of acts of retaliation or discrimination against the reporter for reasons connected, directly or indirectly, to the report; and
- adequate sanctions against those who are in breach of the aforementioned measures to protect the whistle-blower and against those who carry out, with malice or gross negligence, reports that prove to be unfounded.

It is also envisaged that the adoption of the aforementioned discriminatory measures against the reporting officer may be reported to the National Labour Inspectorate, as far as it is responsible, not only by the reporting person but also by the trade union organisation.

As a further protection of the whistle-blower, it is also envisaged that dismissal and retaliatory or discriminatory demotion are invalid and that the burden of proving, in procedural law, that negative measures adopted towards the reporter are based on reasons unrelated to the report.

To align the MOGs with the changes introduced in Decree 231/2001, Italian companies started to update them, providing at the same time a specific whistle-blowing procedure for reporting by employees.

The whistle-blowing procedure should determine specific channels that allow the submission of reports, based on precise and concordant factual elements, guaranteeing the confidentiality of the reporters’ identities.

For a full and effective operation of the procedure, the following measures are considered appropriate:

- the provision of a person able to receive reports, although the law does not provide a specific recipient of alerts;
- the identification of a system of management of violation reports that allows the anonymity of the whistle-blower to be guaranteed;
the specific training of top managers, as well as those subordinated to them; and
the integration of the disciplinary system set up by the MOG, with the inclusion of sanctions against those who violate the protection measures of the reporting person and against those who carry out, with malice or gross negligence, reports that prove to be unfounded.

III ENFORCEMENT

i Corporate liability

Decree 231/2001 regulates the criminal responsibility of corporations with regard to offences committed by their representatives or employees. Even though the Decree provides (formally) for administrative sanctions against corporations, the underlying offence is criminal, and it is in criminal proceedings that the offence is ascertained and the sanction imposed.

It is a criminal court that tries the case and the corporation will have all the defence rights and guarantees of a defendant in a criminal trial. Moreover, this kind of provision certainly responds to the Engel criteria (specifically, the nature of the offence and severity of the penalty), under which the European Court of Human Rights considers a punishment to be effectively criminal, in regard to the need to respect the provisions of the European Convention on Human Rights.7

For the criminal responsibility of legal persons to apply alongside the criminal responsibility of natural persons (representatives or employees), the offence must have been committed in the interests of or for the benefit of the corporation. The exclusive benefit of the agent (or a third party) excludes corporate liability.

Article 5 of Decree 231/2001 states that the corporation is responsible if the criminal offence has been committed by:

- persons holding representative, administrative or managerial positions in the corporation or in any of its organisational units provided with financial and functional autonomy, or persons in charge of managing and overseeing these positions (referred to as senior managers); or
- persons placed under the direction or supervision of any person specified above (referred to as employees).

A corporation may attempt to establish its innocence by providing evidence that the internal organisation of the corporation and its policies and procedures complied with the law and were structured in such a way as to be capable of preventing crimes from being committed.

Originally intended to apply only to offences against the public administration (centred on bribery) or against the assets of the public administration (embezzlement of public money), the responsibility of corporations has been extended through additional legislation to include offences regarding, inter alia:

- public deeds or revenue stamps;
- criminal offences against individuals;
- criminal offences involving market abuse;
- bodily harm or manslaughter because of violations of health and safety regulations;

7 Engel and others v. the Netherlands, 1976, and following cases, including Grande Stevens and others v. Italy, 2014.
receiving stolen goods;

money laundering and the handling of illicit funds and assets;

cybercrime;

organised crime offences;

offences against trade and industry;

criminal offences against intellectual property;

criminal offences against the environment;

fraud against the state or a public body;

corruption;

forgery of money, tax stamps, credit cards and distinguishing marks of industrial products;

corporate crimes;

crimes of terrorism and of subversion of the democratic order;

inducement not to make statements or to make false statements to the authority;

employment of illegal immigrants;

child grooming; and

racism and xenophobia.

One of the most recent developments has been to extend the concept of bribery from bribery of public officers to commercial bribery (bribery of managers of corporations), which is now specifically punished. If the briber acts within a corporate organisation, his or her own company may also be punished (not the company of the bribed, which has suffered damage from the act).

Additionally, as of 1 January 2015, corporate liability has been extended to self-laundering (defined in Article 648-ter 1 of the Italian Criminal Code). Therefore, corporations may be liable if their employees, having committed or participated in committing an intentional crime, employ, replace or transfer, in financial, entrepreneurial or speculative activities, money, goods or other benefits derived from the commission of such a crime, to hinder the identification of their criminal origin. This new provision has had a significant impact on companies that have promptly had to adjust their compliance programmes, including measures to prevent the commission of self-laundering.

With regard to bribery, it should be mentioned that Law No. 3/2019 amending Decree 231/2001 (the Anti-Corruption Law), which aims to strengthen the fight against public corruption and increases the penalties for committing acts of corruption, has added to Article 25 the following:

1. In relation to the commission of the offences referred to in Articles 318, 321, 322, first and third Paragraphs, and 346-bis of the Penal Code, a monetary sanction of up to two hundred shares is applied.

2. In cases of conviction for one of the offences indicated in Paragraphs 2 and 3, the disqualification sanctions provided for in Article 9, Paragraph 2 are applied for a period of not less than four years and not more than seven years, if the offence was committed by one of the persons referred to in Article 5, Paragraph 1, letter (a), and for a period of not less than two years and not more than four, if the offence was committed by one of the persons referred to in Article 5, Paragraph 1, letter (b).

3. 5-bis: If, prior to the first-degree sentence, the entity has effectively taken steps to prevent the criminal activity from having further consequences, to ensure evidence of the offences and
to identify the persons responsible or to seize the sums or other benefits transferred and has eliminated the organisational shortcomings that led to the offence through the adoption and implementation of organisational models suitable for preventing offences of the type of the one that has occurred, the disqualification sanctions shall have the duration established by Article 13, Paragraph 2.

There were some changes to the discipline in 2019: Article 5 of Law No. 39/2019, entitled ‘Offences relating to fraud in sporting competitions, illegal gambling or betting and games of chance exercised by means of prohibited apparatus’, provides that, after Article 25-terdecies of Decree 231/2001, the following is inserted:

Article 25-quaterdecies (Fraud in sporting competitions, illegal gambling or betting and games of chance exercised by means of prohibited apparatus). - In relation to the commission of the offences referred to in articles 1 and 4 of Law 401 of 13 December 1989, the following monetary sanctions are applied to the entity:

a) for offences, the monetary sanction up to five hundred shares;
b) for fines, the monetary sanction up to two hundred and sixty shares.

2. In cases of conviction for one of the offences indicated in paragraph 1, letter a) of this article, the disqualification sanctions provided for in article 9, paragraph 2, are applied for a duration of not less than one year.

Additionally, as of 25 December 2019, corporate liability has been extended to some tax crimes, in application of the Directive 2017/1371 (also known as PIF Directive). The Law No. 157/2019 amending the Decree 231/2001 has introduced the following disposition (Article 25-quinquiesdecies):

1. In relation to the commission of the offences provided for in Legislative Decree No. 74 of 10 March 2000, the following financial penalties shall apply to the entity:

a) for the offence of fraudulent declaration through the use of invoices or other documents for non-existent operations as per article 2, paragraph 1, monetary sanction of up to five hundred shares;
b) for the offence of fraudulent declaration through the use of invoices or other documents for non-existent operations, as per article 2, paragraph 2-bis, the monetary sanction of up to four hundred shares;
c) for the offence of fraudulent declaration through other contrivances, as per article 3, the monetary sanction of up to five hundred shares;
d) for the offence of issuing invoices or other documents for non-existent operations, as per article 8, paragraph 1, the monetary sanction of up to five hundred shares;
e) for the offence of issuing invoices or other documents for non-existent operations, as per article 8, paragraph 2-bis, the monetary sanction of up to four hundred shares;
f) for the offence of concealment or destruction of accounting documents, as per article 10, the monetary sanction up to four hundred shares;
g) for the offence of fraudulent deduction from the payment of taxes, as per article 11, the monetary sanction up to four hundred shares.

2. If, following the commission of the offences indicated in paragraph 1, the entity has made a significant profit, the monetary sanction is increased by one third.
3. In the cases referred to in paragraphs 1 and 2, the disqualification sanctions referred to in article 9, paragraph 2, letters c), d) and e) are applied.

Alongside the criminal or administrative liability under Decree 231/2001, and in addition to any administrative penalties that CONSOB or other authorities may impose, a company may also incur liability under civil law if its directors or employees are held responsible under criminal law. Pursuant to Article 2049 of the Italian Civil Code, a company is strictly liable for all damages caused to third parties by its own employees, representatives or directors, even if these damages are the result of a criminal offence.

The same lawyer may defend both a company and any suspected employee, unless there is a conflict of interest between the two. Only then does the Code of Practice require the counsel to refuse to assist at least one party and not to exploit any confidential information received when defending the other. If, for example, the company’s defence asserts that the offence was committed by the employee in the latter’s own exclusive interest and for his or her own benefit, then obviously, according to the structure of Article 6, the two parties would require different defence counsel. When the company’s defence strategy involves the defence of its staff, that defence will generally be joint or closely coordinated.

ii Penalties

Legislative Decree 231/2001 sets forth four types of penalties: monetary penalties, restrictive penalties, seizure of assets and publication of conviction. The monetary penalties are applied on the basis of units, which cannot be fewer than 100 and not exceed 1,000. The amount of each unit ranges from a minimum of €258 to a maximum of €1,549, which is set at the discretion of the judge based on the severity of the crime, the economic condition of the company and the scale of its assets. (For example, in the case of bribing a public officer, the law indicates a range of between 100 and 800 units and the judge may decide to apply a penalty of 200 units. If the company is large, the judge may apply a value of €1,500 for each single unit and thus the total penalty would be €300,000.) The judge must also consider any activity carried out to cancel or reduce the consequences of the crime.

Apart from monetary penalties, the judge, if expressly established, could also apply restrictive penalties but that would only occur under one of these two conditions: that the entity made a remarkable profit, or that the offence was committed either by a senior manager or by an employee. In the second case, the penalty could be applied only if the offence was committed because of serious organisational deficiencies. In the event of reiteration of offences, restrictive penalties can involve either fines or disqualification, such as:

- a ban on carrying out business activities;
- suspension of licences and concessions;
- a ban on dealing with public bodies;
- exclusion from or cancellation of public financing or contributions; and
- a ban on advertising goods or services.

The above-mentioned Anti-Corruption Law has extensively amended Paragraph 2, Article 13 (on restrictive penalties), to state: ‘Without prejudice to the provisions of Article 25, Paragraph 5, disqualification sanctions have a duration of not less than three months and not more than two years.’
Publication of the conviction can be in one or more journals and include bill posting in the municipality where the entity has its main office. During an investigation, if requested by the public prosecutor, it is possible to impose a ban as a precautionary measure when there is a real possibility of further offences of the same nature being committed by the company.

With regard to precautionary measures, which indicate that the entity is liable for an administrative offence and there are well-founded and specific elements suggesting there is a real danger that offences of the same nature as the one being prosecuted will be committed, the Anti-Corruption Law provided the following:

a. the judge determines the duration of precautionary measures, which may not exceed one year;

b. after the sentence of first-instance conviction, the precautionary measure may have the same duration as the corresponding sanction applied with the same sentence, and the duration of the precautionary measure may not exceed one year and four months;

c. the duration of the precautionary measure must begin upon the order notification; and

d. the duration of the precautionary measure must be taken into account when deciding the duration of the applicable sanctions.

iii Compliance programmes (models of organisation and governance)

The keystone of Decree 231/2001 is the partial exemption from corporate liability that comes with the adoption of an effective and efficient organisational model, capable of preventing predictable offences, established by the ‘gap analysis’.

If the supposed offence was committed by senior management, the burden is on the company to prove that the persons committed the offence by fraudulently evading the effective and appropriate organisation model and the controls in place; however, if the offence was committed by a less senior employee, it is for the public prosecutor to demonstrate a failure to comply with the obligations of direction and oversight imposed on the employee.

Reparatory compliance programmes (i.e., those developed after an offence has been committed) may, on the other hand, entail a reduction in the fine, exemption from the application of bans or the suspension or revocation of precautionary prohibitive measures, or the suspension and subsequent conversion of the fines in the event that the reparatory action was carried out late.

---

8 The mere adoption of the model does not appear to be sufficient to preclude the corporation’s responsibility. As Milan Trial Court stated: ‘the model must have some important characteristics: a deep analysis of the corporation; the ability to find the risky areas for the different types of crimes; and ways to hinder illegal acts, keeping in mind the history [re judiciary] of the company and the characteristics of the other companies that operate in the same sector. The model has to determine what moments in the company are exposed to the risk of crime, study specific procedures to use in those moments that allow for effective control, and use preventive controls and specific protocols to plan the company's decision-making. . . . It must follow the corporation’s changes, updating the model as soon as the risk structure evolves.’ (Court of Milan, Office of the Judge for Preliminary Investigation (G.I.P.), 20 September 2004, IVRlholding-COGEFI). In another decision, the Court of Milan stated that: ‘Effectiveness, specificity and dynamism are structural characteristics of compliance programmes.’ (Court of Milan, Sec. XI, Reexamination Judge, Pres. Mannocci, ord. 28 October 2004, Siemens AG).

9 The Italian government nominated a review commission to empower the efficiency and the aim of prevention of Legislative Decree No. 231/2001.
Article 6, c.2 of Decree 231/2001 establishes the essential characteristics for the organisation, management and control model. The first two activities to be developed are linked to risk assessment, in particular:

a identification of potential risks; and  
b design of the control system: in particular, the guidelines of Confindustria\(^{10}\) establish the most important components to an effective control system as:

- a code of ethics referencing the offences considered;
- a sufficiently formalised and clear organisational system, in particular with regard to the attribution of responsibility;
- allocation of the power of authorisation in accordance with defined managerial and organisational responsibilities;
- a risk management and control system; and
- communication and staff training.

The compliance programmes should also include specific rules of conduct for employees. This code of conduct should be done after the risk assessment and the gap analysis and should establish specific procedures to regulate the decision-making process.

Confindustria has also established some guidelines to comply with Decree 231/2001. In particular, the minimum contents of the compliance programme should establish that:

a the essential principle of the entity should be the respect of law in every country where the entity acts;

b every operation and transaction has to be correctly registered, authorised, verifiable, legitimated, coherent and appropriated; and

c the entity has to establish the basic principles in relation to its commercial partners.

### iv Prosecution of individuals

When an investigation or initial criminal action is directed against a natural person who is an employee or senior manager of a company, it is generally the company that arranges an adequate professional defence for its employee and bears the costs, given the common interests of the company and of the natural person in proving that no offence was committed.

The company and the natural person oppose one another only in a limited number of cases; this mainly occurs when the employee has caused damage to the company when committing the offence, or fraudulently evaded company procedures to commit the offence. In these situations, the company will mainly be interested in dismissing or otherwise sanctioning the employee – thereby distancing itself from the employee’s conduct – and then in joining the criminal proceedings as a civil claimant to obtain compensation for all damages suffered as a result of the unlawful conduct.

---

\(^{10}\) Confindustria is an association representing manufacturing and service companies in Italy. Membership is voluntary.
IV INTERNATIONAL

i Extraterritorial jurisdiction

Pursuant to Decree 231/2001, criminal liability also extends to criminal offences committed abroad, but only if the corporation’s headquarters are located in Italy (and on the further conditions that no action has been taken by the authorities of the country where the offence was committed and that the requirements for the criminal liability of the natural person that has committed the offence concerned are met).

Conversely, if the crime was committed in Italy by a manager or employee of a foreign company, both the perpetrator and the corporation may be pursued under Italian law despite the fact that the main offices of the company are abroad. Pursuant to the Criminal Code, any offence may be deemed to have been committed in Italy (and not abroad) even if a ‘fragment’ of the action or ‘the conception of the offence’ occurred in Italy. A German corporation has been tried for bribery in Italy under Decree 231/2001 and had to enter into a plea bargain, and many foreign corporations are currently on trial or under criminal investigation in Italy (banks involved in the Parmalat bankruptcy case, other banks involved in investigations regarding derivatives sold to public entities, etc.).

Specific crimes, notably insider trading and market manipulation regarding securities traded on Italian markets, may be punished even if entirely committed abroad. Both the individuals and (under Decree 231/2001) the foreign corporation for the benefit of which the crime has been committed will be punished in Italy. Two of the three major ratings agencies, and some of their managers, were on trial in the small southern town of Trani for alleged market manipulation of Italian treasury bonds: the crime was supposedly committed entirely abroad.

With respect to specific types of conduct, in the case of an offence committed by an Italian entity abroad (according to Article 4 of Decree 231/2001), the entity could be accountable under the conditions provided for in Articles 7 to 10 of the Criminal Code. In particular, Article 7 provides that any of the following offences committed abroad are punishable under Italian law:

a) offences against the state;

b) offences of counterfeiting the state seal and use of the counterfeited seal;

c) offences of forging money and public credit cards; and

d) offences committed by public officials with abuse of authority, or violation of the duties inherent to the function or service.

ii International cooperation

Legislation involving judicial assistance in criminal matters is very similar to those in other European Union (EU) Member States, Italy having ratified the relevant international instruments. In this context, a judicial authority that intends to carry out investigations in a foreign state may request the competent authorities of that state to implement them on its own territory.

---

11 Specified under Articles 7 to 10 of the Italian Criminal Code.
12 Court of Cassation No. 11442/2016.
13 See Section V.
14 On 30 March 2017, the court acquitted the ratings agency Standard & Poor and five of its former and current managers of market manipulation charges relating to previous downgrades of the country's sovereign debt.
behalf, performing the acts requested\textsuperscript{15} and transmitting their results to the requesting country. Alongside national legislation, such matters are governed by international conventions\textsuperscript{16} (although bilateral treaties are much more numerous) and by the general provisions of international law, which – where present – prevail over ordinary legislation.

Extradition involves the surrender of individuals by the state in which they are located to another state that has made an appropriate request to place them on trial or to implement a conviction or other measures involving a restriction of their personal freedom.\textsuperscript{17} Italian authorities refuse to allow extradition of defendants abroad:
\begin{enumerate}
  \item when there are grounds to conclude that they will be subject to persecution or discrimination, or other acts amounting to a violation of their fundamental rights;
  \item for political offences; or
  \item in the event that the conduct in respect of which extradition has been requested is punishable by death in the requesting state.
\end{enumerate}

Within the EU, a European arrest warrant is a simplified form of extradition (implemented in Italy by Law No. 69/2005). This measure equates to a genuine judicial decision according to which the national judicial authority at which it is aimed is required to recognise the request for the surrender of a person made by the issuing judicial authority, subject to a summary control that the relevant prerequisites have been met.

The right granted to the General Prosecutor to also request the enforcing state to hand over assets covered by any seizure or confiscation order is significant for companies. Where requested by the issuing authority, the Court of Appeal may also order the seizure of assets required as evidence, provided that they are sizable.

Italy allows extradition to a foreign requesting country even if no specific extradition treaty has been signed. The Code of Criminal Procedure provides framework rules for a non-conventional extradition, basically requesting stricter scrutiny on the grounds for the extradition, if there is serious suspicion of guilt and a risk of discrimination, but an Interpol red alert notice, requesting the arrest of an individual in Italy, under an arrest order issued by whatever country in the world, is likely to be executed.

The United Nations Convention against Transnational Organized Crime was ratified by Italy in 2006.

Finally, the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Strasbourg 1990) provides for forms of investigative assistance in, for example:
\begin{enumerate}
  \item the collection of evidence;
\end{enumerate}

\textsuperscript{15} For example, the hearing of witnesses and accused persons, precautionary seizures and the provision of evidence or documents and other items relating to the offence.

\textsuperscript{16} For example, multilateral conventions such as the European Convention on Mutual Assistance in Criminal Matters (Strasbourg 1959), the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Strasbourg 1978) and the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Strasbourg 2001).

\textsuperscript{17} Extradition (and other jurisdictional relations with foreign authorities) is governed by the European Convention on Mutual Assistance in Criminal Matters signed in Strasbourg on 20 April 1959, and by ‘other provisions of international treaties in force in respect of the state and the provisions of general international law’ (Article 696 of the Italian Code of Criminal Procedure). Only if there is no international law – either treaty law or customary law – or where these are incomplete or contain gaps, will the provisions laid down by the Italian Code of Criminal Procedure apply.
the transmission of information to another state (even where not requested);
the adoption of common investigative techniques;
the elimination of bank secrecy as well as provisional measures such as the freezing of
bank accounts;
the seizure of assets to ensure their retention; and
the confiscation of the proceeds of crime.

In addition, in February and March 2015, Italy signed agreements with Switzerland,
Liechtenstein and the Principality of Monaco on the exchange of information, with a view
to ending bank secrecy and better pursuing Italian nationals who abscond abroad with the
proceeds of tax crimes.

Local law considerations

Criminal law is based on the principle of territoriality and, therefore, the investigative
authorities may carry out any investigations against any person in Italy and use any item
found in Italy as evidence, even when multiple jurisdictions are implicated. The only limit
is provided for by Legislative Decree No. 29/2016: Law 29 has transposed Framework
Decision No. 2009/948/GAI and provided in Italian legislation the international ne bis in
idem principle, concerning persons who have been judged by the jurisdiction of another
Member State. The investigative power of the public prosecutor in Italy is not limited by the
right to confidentiality or the right to bank secrecy, but only by the secrecy granted to specific
classes of professional and official secrets. Consequently, for example, if the public prosecutor
were to find some emails within an Italian company sent by the employees or senior managers
of an associate foreign company, or documentation drawn up by foreign companies that is
potentially useful in a case against Italian persons, there would be no limitation on their use.

On the other hand, should it prove necessary for the public prosecutor to obtain
evidence abroad, letters rogatory – amounting to a request in which one state asks another
to carry out specific acts (communications, notifications or the acquisition of evidence) – are
essential instruments.

YEAR IN REVIEW

The major bankruptcies that have shaken Italy in recent years (and above all, those of the
two major food conglomerates Parmalat and Cirio) have involved criminal offences; the
bankruptcies were the result of actions to plunder corporate resources carried out by senior
managers and the crises that exposed them were primarily market related.

Italian capitalism is still mainly based on the control of listed companies by families
or small groups of connected individuals (hence the description ‘relationship capitalism’, as
opposed to the model of the public company, which is very rare in Italy). In the Parmalat and
Cirio cases, both companies were catastrophically in debt and the controlling shareholders
used fraudulent accounting so as not to lose control of their respective companies, relying

18 The Parmalat case has been split into several different proceedings; the main one has recently been judged
by the Court of Cassation (March 2014), a judgment that resulted in complete confirmation of the
accusations. The Cirio case was judged by the Court of Rome; the Court of Appeal confirmed the decision
in April 2015. The Court of Cassation intervened on 30 January 2018 and annulled it, with reference to
heavily on the issue of bonds that they were not able to honour. In the current trials, prosecutors are also arguing that this was only possible with the complicity of national and international banks.

Other major scandals, such as those that broke in 2005 (the attempted banking takeovers of the Antonveneta bank by Fiorani and the Banca Popolare di Lodi, and of the Banca Nazionale del Lavoro by Consorte and Unipol)\(^\text{19}\) or the more recent case of market manipulation involving the insurance company Fonsai,\(^\text{20}\) can be distinguished from Cirio and Parmalat as there was no subsequent corporate collapse. These cases, however, were also characterised by an excess of power in the company leadership, which exploited the companies to their own ends.

All these cases have one common denominator: the failure of the ‘gatekeepers’. While in the United States, Enron dragged down Arthur Andersen with it, in Italy, Grant Thornton and Deloitte & Touche – two other major auditing firms – were directly involved in the criminal trials for bankruptcy and insider trading relating to the Parmalat affair.

From a criminal law perspective, the public authorities have emerged relatively unscathed from recent major scandals. It is, however, sufficient to read the reports of the hearings by CONSOB commissioners in the trial for insider trading in Parmalat stock to appreciate how, leaving aside any questions of criminal liability, CONSOB’s reputation suffered a heavy blow. Its chairman, who was a witness in court, had to admit that the first request for clarifications sent by CONSOB to Parmalat was made on 9 July 2003, following an article in the newspaper La Repubblica raising doubts about the company’s actual level of indebtedness;\(^\text{21}\) had the article not appeared, CONSOB would probably not have initiated any investigation at that point, as it would not have independently ascertained the level of Parmalat’s financial difficulties.

The Bank of Italy was hit by the scandal following the attempted takeover of Banca Antonveneta by BPL; the former governor has been convicted for market manipulation in collusion with the then-managing director of BPL.\(^\text{22}\) As an institution, the Bank of Italy has emerged stronger from this affair, as the trial has highlighted how officials within the bank worked with the utmost honesty and competence, and were capable of withstanding pressure from the governor of the Bank of Italy, who subsequently resigned as a result of the scandal.

\(^{19}\) Both of which were judged by the Court of Cassation in 2012.

\(^{20}\) The Milan Court of Appeal has confirmed the acquittal of Gioacchino Paolo Ligresti, accused of false accounting and stock manipulation, in relation to the past management of Fondiaria-Sai, of which he was an adviser. The Milan Public Prosecutor’s Office, CONSOB and the consumer movement, with 900 former shareholders of the insurance group, had challenged the acquittal, but at the end of the hearing, the Deputy Attorney General Celestina Gravina requested the acquittal. Giulia Ligresti was acquitted by the Court of Appeal of Milan, which accepted the petition for revision of the first-instance judgment and revoked the first-instance plea agreement of two years and eight months in prison. This was forced after the sentence of acquittal against Paolo Ligresti became final, making the two verdicts ‘irreconcilable’. The indictment of Jonella Ligresti and other managers of Fonsai has been annulled. The trial will begin again in Milan. On 12 March 2019, the first section of the Court of Appeal of Turin accepted the defence that had raised doubts about the territorial jurisdiction of the Piedmontese Court, which on 11 October 2016 had sentenced Jonella Ligresti to five years and eight months in prison.

\(^{21}\) Milan District Court, criminal proceedings 12473/04, hearing of 31 May 2006, p. 162 of the transcript.

\(^{22}\) The judgment became final in the Court of Cassation in 2012.
In the above-mentioned *Fonsai* case – regarding market manipulation and false accounting by the former managers and shareholders of an insurance company – the former head of the Italian Insurance Supervisory Authority was charged with bribery.

This simple point goes to the heart of the system: if the gatekeepers fail, if internal and external auditors are not able to guarantee a minimal level of truth in the company accounts, and if the highest national oversight and control authorities are not able (in the best-case scenario) or not willing (in the worst) to exercise effective control, nothing will prevent the worst behaviour by company shareholders.

Between 2012 and 2018, a significant number of cases of market manipulation came under criminal investigation. Because this crime may be punished even if committed entirely abroad, an Italian public prosecutor could investigate market manipulation allegedly committed by rating agencies\(^{23}\) or by international banks that affected securities traded on the Italian market.

Noteworthy is the recent trend of proceedings for financial and bankruptcy law crimes that concern some of the most important banks. Monte dei Paschi di Siena is currently involved in a trial before the Court of Milan for the crimes of market manipulation, obstruction to the functions of the public supervisory authorities and false accounting.\(^{24}\) Other important banks are involved in criminal proceedings for the crime of bankruptcy: the *Banca MB*,\(^ {25}\) *Banca Etruria*\(^ {26}\) and *Banca Carife (Cassa di Risparmio di Ferrara)*\(^ {27}\) cases are just a few of the most important proceedings.

The same can be said of the most recent cases of market manipulation and false accounting that have emerged during the banking and financial crisis of the past few years: the top managers of Banca Popolare di Vicenza are currently on trial in Vicenza.

**VI CONCLUSIONS AND OUTLOOK**

The legal system's reaction to these financial crises has been left in the first instance to criminal law, with trials that have now been ongoing for years. But can criminal law alone cope with this situation and can it prevent further crises from occurring?

---

\(^ {23}\) As mentioned above, on 30 March 2017, the Court of Trani acquitted the ratings agency Standard & Poor and five of its former and current managers of market manipulation charges relating to previous downgrades of the country's sovereign debt.

\(^ {24}\) Currently, the judges of the Second Criminal Section of the Court of Milan have rejected the plea of territorial incompetence made by the defence, which asked to bring the case back to Siena, where it was originally opened. The judges thus declared the hearing open, with the consequent formulation of their requests for evidence and documentary production.

\(^ {25}\) Ten former executives of the bank are on trial before the Court of Milan. Because of the coronavirus emergency, the trial has been postponed and will begin on 8 October 2020 before the judges of the second criminal section of the court of Milan. The offence of obstruction of the supervisory authority has fallen for prescription, while, of the 18 charges, four cases of bankruptcy remain.

\(^ {26}\) The former executive director of the bank and other former executives are currently under investigation from the office of the Public Prosecutor of Arezzo.

\(^ {27}\) The first-degree trial has been concluded, which saw only two convictions among the 11 defendants for whom the Prosecutor's Office of Ferrara had requested more than 47 years. The other nine were acquitted.
However necessary, criminal law is inherently subsidiary. Given the problem, in the case of Italy, of the inherent tendency of major economic players towards opportunistic behaviour to the detriment of the market, the solution can never, by definition, be left to criminal law alone; it must be integrated into the framework of a comprehensive system of rules.

The first point of order must involve either private law or administrative law alongside some pre-legal regulations such as reputational rules, codes of practice and ethical standards. This is merely a single aspect of a much more complex picture. To prevent opportunistic behaviour by major corporations to the detriment of the market, one possible solution is to put specific gatekeepers on guard, to use a term used by US scholars. Root-and-branch reforms are necessary, not only of criminal law, but also of civil and administrative law. Under such reforms, the role of the gatekeepers – starting with the statutory auditors, the external auditors, and the oversight and control authorities – must be well defined and carried out prior to the initiation of criminal investigations by public prosecutors.

Moreover, their powers of inquiry must be adequately formulated so as to make it possible for the oversight authorities to hear the alarm bells ringing in a timely fashion.

Recent scenarios

The Supreme Court has recently had the opportunity to rule on a matter subject of various interpretations over the years: the application of the rules set out in Decree 231/2001 to foreign-based entities.

The defence of the entity claimed that, because the entity's head office is abroad, the assisted entity should not be called to answer under Decree 231/2001, as no reprimand can be made, deriving from 'organisational fault', to the entity except in the place where it has its decision-making centre.

The Supreme Court, despite the above-mentioned thesis of the defence, has clarified that the entity is liable, like anyone else, regardless of nationality or the place where its head office or its principal place of business is located, if the offence has been committed on Italian territory.

The Supreme Court added, moreover, that the entity is subject to the obligation to comply with Italian law and, in particular, the criminal one, regardless of whether or not there are rules governing in the same way the same matter in the country to which it belongs.

Another important decision concerning the application of the Decree 231/2001 has been issued by the Supreme Court on 27 January 2020 (sentence No. 3157).

The Supreme Court underlines the fact that negligent offences also give rise to administrative responsibility of the company. Therefore, there is an obligation for the entrepreneur to adapt requirements of interest and advantage (indicated by Decree 231/2001, Article 5, Paragraph 1) also in these cases.

The United Sections of the Supreme Court has already issued an important concept in decision No. 38343/2014. According to this orientation, the literal interpretation is the following: the concepts of interest and advantage, in culpable offences, must be referred to the conduct and not to the anti-judicial outcome. The adjustment only concerns the object of

29 Court of Cassation No. 11626/2020.
the evaluation that no longer captures the event but only the conduct, in accordance with the
different conformation of the offence; and without, therefore, any harm to the constitutional
principles of the penal system.

Subsequently, it was reiterated, with reference to culpable offences in the field of safety
at work, that the concepts of interest and advantage should refer to conduct and not to the
anti-judicial outcome:

undoubtedly, they do not respond to the company’s interest, or do not provide the company with an
advantage, the death or injury suffered by one of its employees as a result of violations of accident
prevention regulations, while there is no doubt that an advantage for the company can be seen, for
example, in the saving of costs or time that it would have had to incur to comply with the prevention
regulations, the violation of which resulted in an accident at work.30

Concerning negligent offences in the field of safety at work, the interest and the advantage
are linked to the savings in expenses that the company would have had to incur to comply
with the regulations. Another advantage for the company could be that it saves time by not
applying the precautionary regulation.

The principles abovementioned can therefore also be adapted to culpable environmental
crimes. Also, in this case, the interest and the advantage are to be identified both in the
economic savings for the entity caused by the failure to adopt plants suitable to prevent the
tabular limits being exceeded, and in the elimination of downtime to which the maintenance
of these plants should have given rise.

ii The coronavirus emergency

The recent coronavirus emergency will inevitably lead to consequences of various kinds, even
in the field of criminal law.

First of all, the need to maintain a different lifestyle from the previous one, marked
by social distancing, will allow for experimentation with new ways of conducting hearings.
In particular, the so-far considered hypotheses have paved the way for the conduct of the
hearings in a totally ‘computerised’ way – through the use of videoconferences – creating a
type of criminal trial that until now has been completely unknown.

From a different point of view, we are already seeing and expect to see in future the
opening of investigations by the Public Prosecutors’ Offices of the areas most affected by
the virological phenomenon, to ascertain the criminal responsibility of those facilities, such
as nursing homes and hospitals, with reference to the deaths that occurred in the various
facilities present in that territory. The investigations that will arise will be carried out on
the basis of objections raised pursuant to Decree 231/2001, which provides for the liability
of the entity for multiple criminal hypotheses – as seen above – potentially detectable
in the aforementioned emergency situation (e.g., think of the discipline contained in

30 Court of Cassation No. 24697/2016.
I  INTRODUCTION

As in many other jurisdictions, corporations in Japan must comply with laws relating to their business areas, and to secure the compliance of corporations, the laws provide criminal sanctions and, additionally where a regulatory body exists, administrative sanctions.

Criminal sanctions against corporations constitute economic sanctions such as criminal fines, confiscation and the subsequent collection of money. A caveat is that criminal fines in Japan are generally not severe in terms of monetary amount for large international companies and, therefore, the disadvantage of criminal sanctions for such companies exists mainly in reputation damages and the time and cost burdens of criminal proceedings, which may include requiring a representative director to be present at court.

One of the features of the Japanese criminal justice system is that the sole authority responsible for criminal procedures is the Public Prosecutor's Office (Prosecutor's Office). Therefore, even if a company violates a law of a specific business area that is regularly monitored by another authority, the Prosecutor's Office has the sole authority and discretion to determine whether it will indict the company. When the company is indicted, the case moves to the proceedings at the criminal court.

However, it is not feasible to impose criminal sanctions on every company that committed misconduct because the Prosecutor's Office does not have any regulatory monitoring functions in specific business areas, and it requires considerable time and resources to impose criminal sanctions through criminal court proceedings. Thus, practically speaking, administrative sanctions have an important deterrent role against illegal misconduct by corporations. These administrative sanctions include, typically, cease-and-desist orders and surcharge orders (administrative fines). For example, in bid-rigging and cartel cases, the amount of surcharge is calculated based on the relevant sales amount of the company and, therefore, surcharge orders can potentially become quite large from an economic point of view.

With respect to the power of investigation, the Prosecutor's Office has the authority to conduct a search and seizure as compulsory enforcement, in other words, a dawn raid. This is accomplished with a court’s warrant under the Code of Criminal Procedure. The National Police Agency (NPA) has the same authority. Other authorities, such as the Japan Fair Trade Commission (JFTC), have the authority to conduct an on-site inspection as part
of an administrative investigation. In a legal sense, this kind of inspection is different from the dawn raid conducted by the Prosecutor’s Office or the NPA in terms of the authorities’ coercive power, but in practice, the process is similar.

In almost all cases, a suspected company officially states that it is cooperating with investigation including search and seizure conducted by the Prosecutor’s Office and other authorities. Although arguments on the necessity or scope of search and seizure can be raised by the company, it would be difficult to successfully resist it in practice.

If a company successfully detects possible misconduct in advance of the commencement of the competent authority’s investigation, the company would have to proceed very cautiously with the necessary steps, including an internal investigation process and application of the leniency programme if available. Internal investigation may also be required in certain cases where, for example, the competent authority issues a reporting order for a suspected misconduct, or accounting auditor requires it for the purpose of its opinion on the company’s financial statement.

Typical areas of laws relevant to corporate activities and competent authorities are as follows:

<table>
<thead>
<tr>
<th>Areas of laws</th>
<th>Administrative sanctions</th>
<th>Criminal sanctions</th>
</tr>
</thead>
<tbody>
<tr>
<td>General criminal code (Penal Code) offences (embezzlement, breach of trust, fraud, bribery, etc.)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Act on Prevention of Transfer of Criminal Proceeds</td>
<td>Respective authorities that supervise the industry</td>
<td></td>
</tr>
<tr>
<td>Companies Act (special breach of trust, illegal dividends, benefits, etc.)</td>
<td>Ministry of Justice</td>
<td></td>
</tr>
<tr>
<td>Competition laws such as Antimonopoly Act (cartel, bid-rigging), Sub-Contracting Act, etc.</td>
<td>Japan Fair Trade Commission (JFTC)</td>
<td></td>
</tr>
<tr>
<td>Securities law such as Financial Instruments and Exchange Act (misrepresentation of financial statements, insider dealing, etc.)</td>
<td>Securities Exchange and Surveillance Committee (SESC) and Financial Services Agency (FSA)</td>
<td></td>
</tr>
<tr>
<td>Tax laws such as Income Tax Act, Corporation Tax Act</td>
<td>National Tax Agency (NTA)</td>
<td></td>
</tr>
<tr>
<td>Banking Act, money-lending business law, etc.</td>
<td>Financial Services Agency (FSA)</td>
<td></td>
</tr>
<tr>
<td>Consumer protection-related regulations, such as Act on Specified Commercial Transactions and Act against Unjustifiable Premiums and Misleading Representations</td>
<td>Consumer Affairs Agency (CAA)</td>
<td></td>
</tr>
<tr>
<td>Personal information law, such as Act on the Protection of Personal Information</td>
<td>Personal Information Protection Commission</td>
<td></td>
</tr>
<tr>
<td>Labour law, such as Labour Standards Act</td>
<td>Labour Standards Inspection Office</td>
<td></td>
</tr>
<tr>
<td>Pharmaceutical law, such as Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices</td>
<td>Ministry of Health, Labour and Welfare</td>
<td></td>
</tr>
</tbody>
</table>

As a general rule, the Prosecutor’s Office and the NPA are in charge of all punitive provisions under Japanese law.

II CONDUCT

i Self-reporting

If a company detects illegal corporate activities, the company may obtain certain advantageous treatment from the authority by voluntarily reporting it. Below are some examples.

a The leniency programme under the Act on Prohibition of Private Monopolisation and Maintenance of Fair Trade (Antimonopoly Act, a basic competition law in Japan). Regarding the violation of Antimonopoly Act, there is a legal leniency programme, under which if a company voluntarily declares to the JFTC a case of wrongdoing (for
example, a cartel or bid rigging) that may constitute a violation of the Antimonopoly Act, an administrative fine against the company would be exempted or reduced. This leniency programme was amended in 2019. Specifically, prior to the commencement of the JFTC investigation, a company that ranked first in the timeline of leniency applications would obtain a 100 per cent reduction and a company ranked second would obtain a 20–60 per cent reduction, etc. After the commencement of the JFTC investigation, the reduction percentage becomes smaller, but it is still possible to receive a 10–30 per cent reduction for a company ranking first. The amendment granted the JFTC discretion to decide the actual reduction percentage based on the value of evidence provided by a company.

b Other certain regulatory frameworks also provide a legal leniency programme. For instance, the false advertising law (the Act against Unjustifiable Premiums and Misleading Representations) provides that if a company voluntarily declares a violation to the CAA, it can receive a 50 per cent reduction in surcharge.

c As a general rule under criminal law, if a person who commits a crime declares his or her wrongdoing to the relevant authority before it is discovered, he or she may receive a reduction in the term of imprisonment or the amount of penalty – known as ‘voluntary surrender’ – subject to a criminal judge’s discretion, on the condition that the declaration is made before the authority in question discovers a crime or identifies a suspect. In general, self-reporting may be considered a good reason to reduce a potential penalty, whether it falls under the legal definition of voluntary surrender or not, although it is only a circumstantial factor.

d A new framework for an immunity agreement between a criminal suspect and the prosecutor in charge has been adopted through an amendment to the Code of Criminal Procedure. The new law has been effective from 1 June 2018. Under this new framework, if a criminal suspect provides the information used for another party’s criminal wrongdoing to an investigating agency under an immunity agreement with a prosecutor, he or she may receive beneficial treatment in light of his or her responsibility. See Section V for details.

ii The beginning of the investigation

Typically, a company becomes aware of illegal corporate activities being carried out within the company when the authority initiates an on-site inspection or a dawn raid. An increasing number of cases are being discovered through companies’ internal reporting systems (including whistle-blower systems) or through the provision of information by outside parties. In recent years, quite a few Japanese companies have been implicated in international cases, and some target companies only become aware of illegal activities by receiving a subpoena, a request for information letter or other governmental notice from overseas authorities.

---

2 The amended Antimonopoly Act was published in June 2019 and will be effective by December 2020 (the actual Effective Date has not been decided yet). See: www.jftc.go.jp/en/pressreleases/yearly-2019/June/19061907.html.
iii Internal investigations

As a recently adopted practice, when certain illegal activities are committed within a company, the company establishes a special committee and entrusts it with conducting a fact-finding internal investigation. The investigation committee gathers documents inside the company, interviews relevant employees or third parties and obtains opinions from outside experts. During the process of collecting documents, digital forensic technology is often used.

The members of the investigation committee vary according to the severity of the case (whether the company management is involved, for example) or the degree of social attention. If a company believes the issue is extremely serious and there is potential for public scrutiny, it may appoint an independent third party, such as outside counsel in most cases, and an expert in other professional areas, such as an accountant, to constitute the investigation committee. This is done to ensure objectivity and neutrality. The Japan Federation of Bar Associations (JFBA) issued the Third-party Committee Guidelines for Corporate Misconducts on 15 July 2010, based on the fact that such investigation committees have become popular. However, as the JFBA guidelines set some strict rules and it is not compulsory to adhere to the guidelines, there is a tendency that certain portions of such companies establish investigation committees called Special Committee or Internal Committee and avoid full application of the guidelines. The attorney–client privilege and work-product doctrine are gradually becoming recognised and must be carefully treated in cases where any international aspects exist, because Japanese law generally does not recognise such privileges while there are no strict discovery rules in domestic litigation (see Section III.iv for details).

In the case of a listed company, if the scandal might impact the company’s financial reporting, the accounting auditor would demand the company to establish a special committee investigating the case for the purpose of issuing its opinion. The stock exchange also comes into play concerning the listed company’s response. The Japan Exchange Regulation (JPX-R) issued the Principles for Responding to Corporate Scandals on 24 February 2016. The JPX-R alleged there had been times when some listed companies did not properly respond to their wrongdoings. Under these circumstances, where the interest in wrongdoing is particularly pronounced, the results of an internal investigation are frequently publicly disclosed. As a result, the company controlled by subsequent management might take legal action to seek damage compensation against the former management in cases where the management had been in violation of its duty of care. In addition, shareholders sometimes require managers to resign from their position or to pay damages to the company. Shareholder derivative lawsuits may result.

iv Whistle-blowers

Under the Companies Act, a company with a certain level of capital or assets is required to establish an internal reporting system as a part of its internal control system (Article 100 of the Enforcement Regulations of the Companies Act and Articles 362(4)(vi), (5) of the Companies Act). The contact for an internal reporting system often takes the form of a

---

3 Updated on 17 December 2010.
4 See: www.jpx.co.jp/english/news/3030/b5b4pj0000022x5j-att/responding_20180330.pdf. Subsequently, the JPX-R issued the Principles for Preventing Corporate Scandals on 30 March 2018, based on the following thought: ‘Now that corporate scandals are no longer uncommon, however, there is an imperative need for listed companies to take effective measures to prevent the occurrence of corporate scandals.’ See also: www.jpx.co.jp/english/news/3030/b5b4pj0000022x5j-att/preventive_20180330.pdf.
specific department within a company or a hotline to the office of outside counsel. Thus, the framework that whistle-blowers may use for reporting has been established more broadly. In practice, the number of cases in which corporate scandals are initially detected by internal reporting is rapidly increasing.

As for the protection for internal whistle-blowers, the Whistleblower Protection Act stipulates that an employee should not be dealt with disadvantageously by the employer on the grounds of making an internal report for public interest. Specifically, it prohibits the dismissal or discriminatory treatment of whistle-blowers. To assist companies in establishing internal control systems, the CAA issued new Guidelines for Business Operators Regarding the Establishment, Maintenance and Operation of Internal Reporting Systems Based on the Whistleblower Protection Act of 9 December 2016.5

III ENFORCEMENT

i Criminal procedure

*Investigation by the Prosecutor’s Office or the NPA*

From a legal standpoint, all criminal offences are charged by the Prosecutor’s Office, even if other authorities initiate an investigation or inspection and impose an administrative order. This is the case even for misconduct related to corporate activities. Having said that, as explained in Section I, in the context of illegal corporate activities, the administrative authority that monitors the business regularly would recognise and investigate the case and if it is judged malicious, it would refer the case to the Prosecutor’s Office. For example, the JFTC has referred malicious cases of bid-rigging.

On the other hand, a corporate crime that many people pay attention to or controversial economic cases are handled by the Special Investigation Department, which is a part of the Prosecutor’s Office. For example, the *Olympus* case and the *Nissan* case (see Section V for details) were handled by the Special Investigation Department.

When the criminal investigation is ongoing against the company in addition to the individual employee, it would be typical practice to separate the lawyers representing the company and the individual employee.

ii Administrative procedure

*Investigation by the SESC, JFTC, NTA and others*

The administrative procedure that is conducted by authorities such as the SESC, the JFTC, the NTA and the CAA eventually leads to administrative orders or sanctions, such as a corrective order, cease-and-desist order or surcharge order. Primarily, an administrative investigation is carried out against violations of laws and regulations engaged in through corporate activities.

As compared to the criminal procedure, the administrative procedure targets the company and does not target the individual employees. Therefore, in most cases, it would not be necessary to retain outside counsel to represent individual employees in response to the administrative procedure.

Further, it is possible that those conducting the administrative investigation do not assume (and even dislike the situation) that outside counsel plays a certain role in a company’s

---

response, because the administrative authority may have the mindset that the facts to be reported should not be touched or diverted by outside counsel. However, as obviously the outside counsel is better positioned to help companies under administrative investigation, it would be advisable to consult with counsel on the legal rights of the company, fact-finding activities, accuracy of the company’s description of facts and overall strategy for the company’s response to the authority and other stakeholders.

Based on the constitutional requirement of due process, in principle, evidence obtained during an administrative investigation should not be used for an investigation for criminal cases or other criminal procedure if the case becomes a criminal case.

iii The JFTC’s enforcement

As an example of the latest enforcement activity in Japan, the number of enforcements by the JFTC is illustrated in the following chart.6

<table>
<thead>
<tr>
<th>Enforcement activity</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports of cases of alleged violations of Antimonopoly Act</td>
<td>6,886</td>
<td>6,331</td>
<td>7,224</td>
<td>5,578</td>
<td>3,620</td>
</tr>
<tr>
<td>Cases in which administrative orders were issued as a result of violations of Antimonopoly Act</td>
<td>10</td>
<td>9</td>
<td>11</td>
<td>13</td>
<td>8</td>
</tr>
<tr>
<td>The aggregate amount of surcharge (billion ¥)</td>
<td>17,143</td>
<td>8,510</td>
<td>9,143</td>
<td>1,892</td>
<td>0.261</td>
</tr>
<tr>
<td>Cases of leniency applications under Antimonopoly Act (actually applied cases (only announced))</td>
<td>61</td>
<td>102</td>
<td>124</td>
<td>103</td>
<td>72</td>
</tr>
<tr>
<td>(actually applied entities (only announced))</td>
<td>(4)</td>
<td>(7)</td>
<td>(9)</td>
<td>(11)</td>
<td>(7)</td>
</tr>
<tr>
<td>(10)</td>
<td>(19)</td>
<td>(28)</td>
<td>(35)</td>
<td>(21)</td>
<td></td>
</tr>
<tr>
<td>Cases in which administrative orders were issued as a result of violations of the Sub-Contracting Act</td>
<td>7</td>
<td>4</td>
<td>11</td>
<td>9</td>
<td>7</td>
</tr>
</tbody>
</table>

With regard to violations of the Antimonopoly Act, the overall number of cases and the amount of surcharges are decreasing. This decreasing trend is mainly because companies have become more aware of the risks of violating the Antimonopoly Act. The JFTC is shifting its resources to enforcing violations of other categories of regulation.

iv Local law considerations

Under Japanese law, there are no privilege doctrines per se, such as attorney–client privilege or attorney work-product, that may be used as defensive measures against an authority’s investigation. Because there are no rules that particularly focus on this issue, communications between attorney and client are not legally protected. In addition, attorney work product is not necessarily protected regardless of whether they were prepared in anticipation of litigation, although there are a lot of current arguments that the protection of privilege should be expanded.

In March 2019, the JFTC announced that attorney–client privilege will be adopted in the JFTC rules at the timing of the effective date of the next amendment to the Antimonopoly Act, which was published in June 2019 and will be effective by December 2020. Currently,

---


7 In the JASRAC case (12 September 2013), the Tokyo High Court judged that under the existing legal system in Japan, the rights and the doctrine under attorney–client privilege or work-product could not be recognised.
this attorney–client privilege rule in the JFTC rules will only apply to cases under the JFTC’s administrative procedure of its investigation regarding violation of a certain category of the Antimonopoly Act.

Other than this, some substantially equivalent rights to protect attorney–client communications are provided under Japanese law. The Code of Criminal Procedure provides the right of refusal against confiscation, particularly based on the expert’s duty of confidentiality.8 Further, in civil proceedings, a party has the right of refusal against production of documents on the grounds of ‘internal use’.

There are no comprehensive disclosure requirements during civil proceedings such as the ‘discovery’ (or, disclosure) procedure often seen in common-law jurisdictions. Although a class-action system has been partly adopted, it is still not considered to have a substantial impact on corporate activities because the plaintiff must be limited to the Specified Qualified Consumer Organisation: a corporation certified by the Prime Minister pursuant to the Consumer Contract Act and the Act on Special Measures Concerning Civil Court Proceedings for the Collective Redress for Property Damage Incurred by Consumers and claims are limited to those concerning consumer contracts.

IV INTERNATIONAL

i Basic framework under the Japanese Penal Code

The Penal Code stipulates the jurisdictional scope of Japanese criminal law (Articles 1 to 4-2). As a general rule, criminal law applies to domestic crimes, and to foreign crimes if there is a special provision by which the authority may reach any particular crimes committed overseas.

If any part of the crime is committed within the geographical confines of Japan (including Japanese vessels and aircraft), Japanese criminal law is applicable. This adheres to the basic principle of jurisdiction.

If any part of the crime is committed outside Japan territory, it is deemed a ‘foreign crime’. Foreign crimes are not subject to Japanese criminal law unless there is an applicable special provision. The Penal Code stipulates several special provisions for foreign crimes to which the Act is applicable (Articles 2 to 4-2), as follows:

a. those who commit crimes concerning the sovereign rights of Japan;

b. a Japanese citizen who commits a crime abroad;

c. those who carry out criminal offences against Japanese citizens abroad;

d. a public officer who commits a crime abroad; and

e. foreign crimes committed under a treaty.

ii International cooperation

The Act on International Assistance in Investigation and Other Related Matters stipulates a framework of coordination with foreign authorities. In addition, there are a number of criminal assistance treaties as bilateral treaties.

The NPA is a member of Interpol and is engaged in international investigation cooperation. International coordination in criminal investigations is made through Interpol or through a diplomatic route (from the local police office to the relevant foreign ministry, and then to the relevant foreign diplomat). In 2019, the total number of instances of

8 Experts include an attorney, doctor, nurse, midwife and patent attorney.
exchange of information through Interpol was 78,114. There were 1,545 Interpol requests for investigation assistance and cooperation from foreign countries to Japan, and 38 via diplomatic routes. The NPA requested assistance from foreign countries in 424 instances via Interpol and on 186 occasions through diplomatic channels.9

iii Extradition
The Act of Extradition governs the relevant issues regarding extradition of a criminal offender to foreign countries. Japan has concluded the Treaty on Extradition as a bilateral treaty with only the United States and South Korea.

The Japanese government will promise to extradite a criminal offender to the United States at the request of the US government if certain criteria are met. The general requirements are that the crime is committed in Japan or the United States, and that penalties can be imposed in Japan and the United States. In a case where the criminal is a citizen of one country, it is not obligatory to extradite him or her to the other country. It is at the discretion of the government to decide whether or not he or she should be extradited. Thus, if the criminal is a Japanese citizen, it will be at the discretion of the Japanese government as to whether it would respond when an extradition is requested. Consideration will be given to the nature of the crime, the influence exerted, the possibility of punishment being imposed in Japan, the level of trust in the international community and national sentiment.

iv Extraterritorial application of the Antimonopoly Act
The JFTC takes the view that if a foreign company is exporting products to Japan and its activities are sufficient to constitute a violation of the Antimonopoly Act of Japan, it is considered to be subject to the jurisdiction of the Antimonopoly Act. For the purposes of sanctions, it is not necessarily required to have a branch office or subsidiary within Japan. Thus, foreign companies may be subject to the Antimonopoly Act if they conduct anticompetitive activities that may impede competition in the Japanese market.


V YEAR IN REVIEW

i An amendment to the Code of Criminal Procedure
In 2016, the Code of Criminal Procedure was amended and the immunity agreement system was newly adopted (as stated at Section II.i, bullet e). By executing an immunity agreement with the Prosecutor's Office, a criminal offender can receive leniency concerning its own crimes by providing information to prosecutors about the criminal acts of others. The new law was effective from 1 June 2018.

The key points of the new system are:

a that a confession of his or her own crime is not necessary; in other words, the system differs from a guilty plea under US law;

b that the crimes regarding which the new system will be used are limited to certain categories. Corporate crimes, violations of antitrust law, tax law violations, violations of the securities law and bribery are applicable crimes;

the court will not get involved in this agreement; 
the content to be included in the agreement is limited in the law; and 
a defence lawyer is required.

In June 2018, Mitsubishi Hitachi Power Systems, Ltd (MHPS) became the first company to which the immunity agreement system was applied in Japan. Consequently, the Prosecutor’s Office charged only two former officers and one former manager of MHPS on suspicion of bribery to a foreign public officer (violating the Unfair Competition Prevention Act). MHPS has not been indicted.

On 19 November 2018, Carlos Ghosn, a former representative director and chairman of Nissan Motor Co, Ltd (Nissan), and Greg Kelly, a former representative director of Nissan, were arrested for violating the Financial Instruments and Exchange Act (FIEA) (namely for making false disclosures in annual securities reports) and indicted on 10 December 2018. It has been reported that an officer and a manager of Nissan entered into immunity agreements with the Prosecutor’s Office and submitted evidence to the Office.

ii Remarkable corporate crime cases

Olympus

Olympus Corporation, a manufacturer of precision machineries and instruments, had been concealing losses of more than ¥100 billion that derived from its financial investment activity and was accused of misrepresenting its financial statements. The company set up a Third-Party Investigation Committee, which issued a report in December 2011. In July 2012, the FSA issued a surcharge order of ¥190 million against the company, based on the result of the SESC’s investigation. The former directors were sentenced to imprisonment with suspension in July 2012, as the SESC also referred the case to the Prosecutor’s Office. In addition, the company filed a civil lawsuit against the former directors. In a relatively recent development, on 16 May 2019, the Tokyo High Court ruled that the former management should be liable for damages of approximately ¥59.4 billion incurred by Olympus.

Toshiba

On 12 February 2015, the SESC issued a request for a report to Toshiba Corporation (Toshiba). Toshiba formed a special investigation committee, and then a third-party committee based upon the fact that there was doubt regarding part of the accounting process – the ‘percentage-of-completion method’ – in regard to the infrastructure projects. While Toshiba voluntarily disclosed the investigation report in July 2015, the Tokyo Stock Exchange requested that it should pay a penalty owing to a breach of covenants that a listed company should follow. On 7 December 2015, the SESC issued an administrative order that imposed a surcharge of ¥7.37 billion on Toshiba. In the face of a series of scandals, Toshiba has filed a lawsuit seeking payment of damages for a total of ¥3.2 billion against former members of management. Counter to that, 36 lawsuits seeking payment of damages for a total of approximately ¥174 billion have been filed against Toshiba.10

---

KOBELO

In October 2017, Kobe Steel Ltd (KOBELO), a major steel manufacturing company, announced that it had engaged in data falsification concerning its aluminium products, copper and other steel-related products over a period of many years. KOBELO’s materials were delivered to other major manufacturing companies, including Mitsubishi Heavy Industries, IHI and Subaru. The chairman and the president of KOBELO resigned from their positions in March 2018 to take responsibility for not detecting the problems.

Nissan

On 19 November 2018, Carlos Ghosn, a former representative director and chairman of Nissan, and Greg Kelly, a former representative director of Nissan, were arrested for violating the FIEA. Ghosn, Kelley and Nissan as a legal entity were indicted on charges of violating the FIEA on 10 December 2018. The Prosecutor’s Office alleged the underreporting of Ghosn’s remuneration as a Nissan director in past annual securities reports. Ghosn was also arrested for aggravated a breach of trust based upon the allegation that Ghosn embezzled Nissan’s money by using several foreign investment vehicles and using them for his personal benefit.

It was reported that Nissan conducted an internal investigation on the alleged misconduct of top management and voluntarily contacted the Prosecutor’s Office. However, Nissan was indicted together with Ghosn and Kelly, and they strongly denied the charges. As widely reported, Ghosn was smuggled out of Japan to Lebanon on 30 December 2019. The criminal procedure against Ghosn was cancelled because the criminal trial needs the accused present at the court.

VI CONCLUSIONS AND OUTLOOK

As stated above, with respect to corporate activities, an administrative sanction may have an effect on a company’s operation, and cases are sometimes referred to the Prosecutor’s Office that then develop into criminal prosecutions. More recently, companies have been voluntarily establishing special committees to conduct internal investigations when a case comes to light. As a cultural tendency somewhat unique to Japan, strong social criticism against companies involved in corporate wrongdoing may seriously impair an entity’s viability as a going concern. Thus, once a company finds itself embroiled in a public scandal, it must proceed with an internal investigation and the other necessary steps with exceeding caution and in close partnership with experienced legal counsel.
Chapter 18

POLAND

Tomasz Konopka

I INTRODUCTION

Depending on the nature of the legal violation, the investigation or control proceedings may be conducted by law enforcement bodies or administrative bodies.

Criminal investigations are, as a matter of principle, carried out by a prosecutor’s office, as it is the key obligation of each prosecutor’s office to maintain law and order and prosecute crimes. In particular, the purpose of the investigation is to establish whether a crime has been committed, the identity of the perpetrator, and subsequently – if the evidence collected appears to prove fault and perpetration – to file an indictment. The prosecutor’s office should also make sure that no indictment is filed against an innocent person; in such an event, the case should be annulled.

The prosecutor is obliged to launch an investigation where there is a justified suspicion of a crime having been committed. An investigation may be launched ex officio or at the initiative of the notifying or the aggrieved party, who must submit a formal (oral or written) notification. For the institution of proceedings with respect to certain crimes, the aggrieved party must file a motion for prosecution. After such a motion has been filed, the proceedings are conducted by enforcement bodies, but it is the aggrieved party that decides whether it wants the perpetrators of the crime to be prosecuted. A motion must be filed for the prosecution of certain business crimes, such as mismanagement (if the State Treasury is not the aggrieved party), or the use of someone else’s business secrets in one’s own business. If no such motion is filed, then no proceedings will take place.

Since 2016, the prosecutors’ offices have operated under new organisational rules. The separation that had previously existed between the position of the Minister of Justice and the Attorney General’s Office has been removed. The tasks of the Attorney General’s Office have been taken over by the National Prosecutor’s Office, headed by the Deputy of the Attorney General’s Office – the National Prosecutor. The place of the appeal prosecutors’ offices has been taken by the regional prosecutors’ offices, which will deal with organised business crime and tax crimes.

An exception has been introduced in the regulation that provided for the independence of individual prosecutors, which provides that a prosecutor is obliged to comply with the directives, instructions and orders of the superior prosecutor (who could be the regional or national prosecutor). Orders may concern the content of the tasks carried out in a specific case.

---

1 Tomasz Konopka is a partner at Sołtysiński Kawecki & Szlęzak.
Crimes are also identified and prosecuted by the police, who have powers to institute preparatory proceedings for less serious crimes; investigations carried out by the police are supervised by a prosecutor. In addition to the police, the power to prosecute crimes is also enjoyed by the Internal Security Agency, the Central Anti-corruption Bureau, the Central Investigation Bureau, the Border Guard and bodies authorised to conduct preparatory proceedings in cases for fiscal offences (within the framework of the National Tax Administration – tax offices, tax administration chambers, tax and customs offices). The other enforcement authorities, as a rule, enjoy the same rights and are bound by the same obligations as the police in criminal proceedings. Nonetheless, particularly risky operations (such as dawn raids) are usually performed either by specialised police units or one of the above agencies.

The Code of Criminal Procedure states that business entities must assist law enforcement bodies upon request. Over the course of an investigation, a law enforcement body may request that a business entity voluntarily provides documents that could represent evidence in the case. If the release of the documents is denied, they are most frequently secured through a search, but law enforcement bodies are not able, for example, to impose a fine for lack of cooperation. An alternative approach may be adopted if criminal proceedings are being obstructed by the perpetrator of a crime being helped to avoid criminal liability. Concealing or destroying evidence that supports the suspicion of a crime constitutes a separate criminal offence and the perpetrator is subject to a penalty of imprisonment for between three months and five years. The same penalty is imposed for any obstruction of criminal proceedings with an intent to assist a perpetrator and help him or her avoid criminal liability. Therefore, one should distinguish between instances of limited cooperation during which account is taken of company interests (for example, by demanding that the bodies respect company secrets) and the aforementioned crime.

Whether an adversarial stance towards the enforcement authorities is a real possibility depends on the specific circumstances of each case and the kind of offence being prosecuted.

II  CONDUCT

i  Self-reporting

Polish law does not provide for the obligation to self-report in relation to committing crimes. Significantly, this lack of obligation to self-incriminate is one of the key principles of criminal proceedings. Given that criminal liability may only be incurred by individuals, this principle is not directly applicable to business entities.

The obligation to report that an offence has been committed only applies to situations in which crimes have been committed by other parties, and this relates to serious crimes prosecuted under the Criminal Code or those that will harm national security. As regards any other types of crimes, the criminal procedure provisions do not provide for a sanction for failure to report them; in particular, Polish law does not provide for a general obligation to report internal irregularities in business entities to the authorities.

With respect to fiscal crimes, it is only possible for the person responsible for committing the act to avoid criminal fiscal liability by making a ‘voluntary disclosure’ or adjustment to a tax return. The Penal Fiscal Code stipulates a number of specific requirements for acts of ‘repentance’ that need to be met for any actions to avoid liability to be effective.

Although not exactly a self-reporting obligation, there is an obligation to report to the General Inspector of Financial Information any transactions that may represent acts of money
laundering. As regards leniency measures in competition law, the competition authority might reduce the amount of the administrative penalty or even decide not to impose such a penalty on an entity that entered into a competition-limiting agreement if that entity submitted an appropriate petition and fully disclosed all important facts regarding said agreement. Full and immediate disclosure and full compliance are required. The disclosing entity is also obliged not to disclose the fact that the petition has been submitted, in particular to the other parties to the agreement in question.

ii Internal investigations

Polish law does not directly provide for the obligation to carry out internal investigations once managers receive information about irregularities within an enterprise, nor is there any obligation to report the results thereof. It is assumed, however, that conducting an internal investigation represents fulfilment of the obligation to take care of the interests of the enterprise under management. Failure to verify signs of irregularity may represent grounds for liability for damages and, in extreme cases, for criminal liability for mismanagement. Internal investigations are conducted not only when the provisions of law have been violated to obtain benefits for the enterprise but also when, as a result of the law being violated, the enterprise has been harmed.

Notwithstanding the above, specific entities (e.g., banks, investment funds, entities managing alternative investment companies, insurance companies, reinsurance companies, as well as entities conducting brokerage activities and fiduciary banks) are obliged on the basis of special provisions to maintain tight compliance control or an internal audit system. These systems have a similar function to internal investigations and are, at times, subject to compulsory reporting. Failure to properly maintain the aforementioned systems may result in one or more of many administrative sanctions being imposed on the entity. Moreover, the Act on Money Laundering and Prevention of Financing Terrorism puts an obligation on entities such as banks, other financial institutions and even law firms to introduce internal procedures to prevent money laundering and the financing of terrorism.

As internal investigations are not regulated, the course of an investigation in either of the situations described above will not differ considerably; however, substantial differences appear when law enforcement bodies institute official investigations or a company decides to report existing irregularities. The enterprise may obtain the status of aggrieved party and enjoy the attributable rights within preparatory proceedings and, at a later stage, court proceedings, if an indictment is filed. These rights include inspecting the case files, participating in the investigation (i.e., participation in witness hearings), and appealing disadvantageous decisions made during the proceedings (such as a decision to discontinue the proceedings). At the court stage, an aggrieved party may act as auxiliary prosecutor to, inter alia, demand compensation of damages or a particular penalty.

In recent years, the number of internal investigations regarding irregularities in the private sector has increased noticeably. In many instances, this is owing to the operation in Poland of companies regulated by the strict rules of the US Foreign Corrupt Practices Act, the UK Bribery Act or French SAPIN II. Moreover, many Polish companies that operate in Germany will have to comply with German law. Germany is likely to adopt strict anti-corruption legislation in 2020 and may became one of the leading European countries in the fight against foreign corruption.

Commonly, an internal investigation will encompass a review of business email correspondence and electronic files, meetings with employees, and of the company's financial
and contractual documents. As regards confidentiality and secrecy, no specific regulations exist and, therefore, use of any information within an internal investigation must comply with generally applicable provisions (especially the EU General Data Protection Regulation). Processing of personal data (except sensitive data) is generally permitted within an internal investigation. However, obtaining the necessary consent from the person to whom the data relates is recommended.

### Whistle-blowers

As it stands, Polish law does not impose a sufficiently general regulation on whistle-blowing. However, employees who disclose irregularities or other undesirable circumstances within an organisation enjoy protection from any resulting discriminatory treatment by employers and managers, although this does not guarantee that a whistle-blower will not suffer negative consequences.

The provisions of the Labour Code do not provide any special protection for people who, in their capacity as employees, have been involved in illegal activities. The employment contract of a whistle-blower who has been involved in criminal activities may be terminated under ordinary procedures or even under dismissal procedures, depending on the circumstances of the case, even though that person reported the irregularities, as long as the treatment of the employee is not discriminatory. Therefore, it should be considered that regulations protecting whistle-blowers are missing from the Labour Code, and thus, in many situations, potential whistle-blowers will not have any incentive to disclose irregularities. Nonetheless, numerous firms have adopted measures to allow anonymous reporting of irregularities noticed within firms. Sometimes, anonymous hotlines or email boxes are made available through which employees can point out violations of law or ethical standards. Despite these efforts, the number of confirmed whistle-blowers in Poland has so far not been significant.

Notwithstanding the above, the whistle-blowing issue is at the stage of appearing under Polish legislation. Pursuant to the Act on Money Laundering and Prevention of Financing Terrorism, some specific institutions are obliged to create an anonymous whistle-blowing procedure of reporting irregularities in the scope of money laundering by employees.

Banks in Poland are obliged to adopt formal whistle-blowing procedures, including an indication of the management board member responsible for handling matters related to whistle-blowing. A bank's whistle-blowing policy is subject to periodic internal assessment.

In November 2019, an amendment was passed to the Act on Public Offering, the Conditions Governing the Introduction of Financial Instruments to Organised Trade, and on Public Companies. It provides an obligation on any legal entity that issues or proposes to issue securities to have procedures for anonymous employee reports to a designated member of the management board, and in special cases, to the supervisory board, of violations of the law, in particular of the provisions of Regulation 2017/1129 of the European Parliament and of the Council of 14 June 2017, procedures and ethical standards.

Pursuant to the textbook of Best Practice of the Warsaw Stock Exchange, it is recommended that companies should organise appropriate systems for reporting irregularities. Poland is also obliged to implement Directive 2019/1937 of the European Parliament and of the Council on the protection of persons reporting on breaches of EU law by 17 December 2021. Pursuant to the provisions of the Directive, internal reporting channels and procedures should meet the minimum standards; in particular, guaranteeing the confidentiality of the identity of the reporting person, which is a cornerstone of whistle-blower protection. The Directive also requires that the person or department competent to receive the report diligently follows it.
up and informs the reporting person within a reasonable time frame about such follow up. Moreover, the entities having in place internal reporting procedures are required to provide easily understandable and widely accessible information on these procedures as well as on procedures to report externally to relevant competent authorities.

When it comes to criminal liability, a person disclosing information to law enforcement bodies regarding crimes and the circumstances of the perpetration thereof may expect extraordinary mitigation of punishment. If a perpetrator discloses to law enforcement bodies previously unknown circumstances relating to a crime that carries a penalty of more than five years’ imprisonment, he or she may submit a motion for extraordinary mitigation of punishment or even a conditional suspension thereof. Furthermore, in the event of corruption in business and in the public sector, a perpetrator of ‘active’ corruption is not subject to penalty if, after the fact of the corruption, that person notifies law enforcement bodies and discloses all significant circumstances of the deed, and all this takes place before law enforcement bodies have become aware of the facts.

III ENFORCEMENT

i Corporate liability

The current Act on Liability of Collective Entities for Acts Prohibited under Penalty, which regulates issues of quasi-criminal liability of commercial companies, has been in force since 28 November 2003. The Act is applicable if a person acting in the name of a company has committed one of the crimes specified in the Act and the company gained, or could have gained, any benefit from this act, whether financial or not.

The list of crimes, the commission of which may cause the commencement of criminal proceedings, includes:

- mismanagement;
- corruption in business;
- credit and subsidy fraud;
- money laundering;
- crimes linked to making repayment of creditors impossible and reducing their satisfaction;
- failure to file a bankruptcy petition on time;
- insider trading; and
- public corruption.

Numerous other crimes are specified in other pieces of legislation that regulate specific areas of economic activity.

A condition for commencing proceedings against a company is that it has been established by a legally final guilty verdict that a crime has been committed by a person acting in the name of a company. There are two other instances when proceedings against a company may be commenced: a verdict that conditionally discontinues criminal proceedings against such an individual, or a verdict that discontinues criminal proceedings by stating that despite the crime having been committed, the perpetrator cannot be punished. Corporate quasi-criminal liability always stems from criminal personal liability.

Liability on the basis of the above-mentioned Act may be imposed in the event that one of the following is proven: (1) at least a lack of due diligence in the choice of the person representing the entity, who is also the perpetrator of an offence; or (2) poor organisation of
the company, which did not ensure the avoidance of the commitment of an offence, which could have been prevented if the body or representative of the collective entity had applied the required due diligence.

The liability arising under this Act is non-transferable; that is, in the case of a merger, division or restructuring of the relevant company, the liability expires. However, the court might impose an interim prohibition on such transformations at a company to prevent it from avoiding.

It follows from practice to date that the law enforcement bodies do not commence proceedings in every case in which such a possibility arises. The Ministry of Justice statistics show that only a couple of dozen proceedings of this type are commenced each year. This figure is very low, especially taking into account the fact that more than 10,000 people are sentenced each year for committing business crimes.

As regards criminal proceedings, although in the strict sense a company cannot be the accused, during the course of proceedings it is nonetheless possible to hand down a judgment ordering a company to reinstate any benefits gained as the result of a crime committed by an individual. In this case, the company becomes a quasi-party and may defend itself against liability by availing itself of certain rights to which the accused is usually entitled. An entity obliged to return benefits has the right to study the case files of the proceedings, may take part in the hearing before the court, file motions to admit evidence, put questions to the witnesses, and appeal unfavourable decisions and verdicts.

In turn, in such proceedings the company may face auxiliary liability. An entity that is liable on an auxiliary basis is liable for a fine imposed on the perpetrator of a fiscal crime if, when committing the crime, the perpetrator acted in the name of the company, and the company gained or could have gained financial benefit.

As regards representation, the original perpetrator and the corporate entity may be represented by the same attorney or counsel, even though its role would be slightly different in each of these proceedings.

ii Penalties

The Act on Liability of Collective Entities for Acts Prohibited under Penalty provides for the possibility of a judgment with regard to a company, imposing a fine of between 1,000 zlotys and 5 million zlotys (but that cannot exceed 3 per cent of the revenue gained in the year in which the crime that forms the basis for liability was committed). The court will mandatorily order the forfeit of any financial benefits gained from the crime, even indirectly.

In addition, the following punishments are possible with regard to collective entities:

a a ban on promotion and advertising;
b a ban on availing of public aid;
c a ban on availing of aid from international organisations;
d a ban on applying for public tenders; and
e making public any information about the judgment handed down.

In the event of auxiliary liability for a tax crime, the scope of liability is determined by the amount of the fine imposed on the accused. Essentially, fines for a fiscal crime range to 24,960,960 zlotys; these amounts change each year in line with the increase in the minimum wage. In ruling practice, however, it is very unusual for fines to exceed 100,000 zlotys.

As regards administrative liability, the amount of fines and the spectrum of other sanctions (revocation of licences or concessions) significantly varies depending on the
relevant duties and legal bases for their imposition. Administrative fines might be very severe, capped at 10 million zlotys (much more than the maximum possible criminal fine) or up to 10 per cent of yearly revenue in the most extreme cases. There is no uniform regulation of administrative sanctions in the Polish legal system.

iii Compliance programmes

At present, legal provisions do not impose the obligation on business entities to implement compliance programmes; however, many firms operate such programmes. They are particularly common in companies with foreign capital and in the financial sector.

The Act on Money Laundering and Terrorism Financing Prevention obliges only specific entities to appoint a compliance officer who will be responsible for supervising the appropriate application of the Act.

Pursuant to the textbook of Best Practice of the Warsaw Stock Exchange, creating and supervising a compliance system is part of the duties of the company’s management board and supervisory board.

A functioning compliance programme is helpful in cases of actions contrary to the law that harm the interests of enterprises. A frequent problem that arises in criminal proceedings involving crimes harming enterprises is the lack of internal regulations clearly laying down the procedures and scope of duties, as a result of which it is difficult to show the actions or omissions of the guilty party.

In the absence of a general regulation of compliance, it would be difficult to establish any specific recommended elements of compliance programmes. As a rule, it would be advisable for the scope of such programmes to cover all branches and subsidiaries of a given entity and ensure regular reviews of their activity. Shortcomings to that extent usually have a very strong negative effect on the efficiency of compliance programmes. The preferred course of action tends to be to involve accounting and auditing experts.

iv Prosecution of individuals

As has already been mentioned, the position of a company in proceedings conducted by law enforcement bodies against an individual depends to a large extent on whether the company gained any benefit from the crime or whether it was harmed by the crime.

At present, the Code of Criminal Procedure provides that an aggrieved party is an entity whose interests have been directly harmed or threatened by a crime. Not every crime that results in an enterprise suffering damage will allow it to exercise its rights as an aggrieved party in criminal proceedings.

On the other hand, provisions of the Code of Criminal Procedure grant a firm the right to appeal a decision by the prosecutor to discontinue an investigation if the firm notified the prosecutor about a crime that harmed its interests, even if only indirectly. To date, only a directly aggrieved party has had the right to file a complaint against decisions on discontinuing an investigation, whereas a person indirectly aggrieved has not had the right to any control over the court. The new regulation should be viewed positively as it grants greater litigation guarantees and may lead to more effective crime prevention.

If proceedings against an individual involve a breach of law that may lead to a company being held liable, a question arises as to the legitimacy of cooperation between the accused and the firm. In the vast majority of cases, a judgment that is favourable to the accused rules out the risk of sanctions for the firm. There are no prohibitions whatsoever on joint defences, so cooperation within the proceedings is admissible. However, situations may arise when the
accused’s line of defence will not be consistent with the interests of the firm. This may be the case, for example, when the accused bases his or her defence on implicating another company employee or manager who is indeed guilty of committing a crime.

The basic duty of the lawyer towards a client in criminal proceedings is to act exclusively for his or her benefit. Pursuant to the position of the judiciary and doctrine that has dominated for years, a defence lawyer must disclose all circumstances that are favourable to the client, even if the client does not consent to this himself or herself.

As regards employee issues, the commission of a crime undoubtedly entitles an employer to terminate the employment contract under a disciplinary procedure. What is important is that the reasons for termination of the contract should be precisely indicated in the written termination of the employment contract, and these reasons can be verified by the court if the employee appeals to the Labour Court. If the reasons given in the termination of the contract prove groundless, the employee may be reinstated by the court or may be entitled to a compensation claim, or both.

As regards payment of legal fees, there are no specific regulations that would prohibit any company from covering the costs of legal services rendered to its employee or a member of its body.

IV INTERNATIONAL

i Extraterritorial jurisdiction

The provisions of criminal law essentially provide for liability for crimes committed in Poland. Pursuant to the provisions of the Criminal Code, a crime is deemed to have been committed at the place the perpetrator acted or omitted to perform an act he or she was obliged to perform, or where the effects of the crime were felt or were intended to occur.

With regard to crimes committed abroad, the rule of the ‘double criminality’ of an act applies. This means that law enforcement bodies may conduct criminal proceedings only with respect to acts that constitute a crime both in Poland and in the country in which they were committed. Polish citizens are liable for crimes committed abroad in all instances where an act constitutes an offence under Polish law and at the place it was committed. As regards foreigners’ liability for acts committed abroad, Polish criminal law may be applied if a crime harms the interests of Poland, a Polish citizen or a Polish company, and at the same time the requirement of double criminality is satisfied.

The requirement of the double criminality of an act does not apply to, inter alia, a situation in which a crime harms the national security of Poland or its material economic interests, or is aimed against Polish offices or officials, nor does it apply to a situation in which financial gain (even indirectly) was derived in Poland.

ii International cooperation

Polish law enforcement bodies cooperate with the authorities of other countries. The rules and scope of cooperation vary, however, in view of the fact that in some cases of cooperation, bilateral international agreements, multilateral conventions or international organisation regulations (including primarily European Union law and its implementations, for example, regarding the Directive 2014/41/EU of the European Parliament and the Council of 3 April 2014 or Council Framework Decision 2009/948/JHA of November 2009) will apply with some countries. In the absence of an international agreement, the provisions of the Code of Criminal Procedure will apply.
The possibility of handing over a Polish citizen as part of an extradition procedure is, in principle, excluded. By way of an exception, the court may decide to extradite a Polish citizen if such a possibility follows from an international agreement ratified by Poland. An additional condition is that the crime with which the subject of the extradition procedure is charged must have been committed outside Poland, and that the act that the person is charged with must constitute a crime under Polish law, both at the time the court decision is made and at the time the crime was committed.

Polish enforcement authorities routinely cooperate with the authorities of a significant number of countries, including Germany and the United Kingdom, mainly as a result of the large Polish populations in those countries.

iii Local law considerations
Enforcement authorities apply the relevant Polish standards in all kinds of proceedings conducted in Poland. The personal data protection regime and the bank secrecy regime are relatively strict and involvement of a foreign element in a given case does not lead to the relevant requirements being loosened in any manner.

V YEAR IN REVIEW
The current government continues its relatively radical efforts to eradicate widespread value added tax (VAT) fraud and other kinds of business crime. One of the revisions introduced a ‘split payment’ system to separate net payments from VAT payments in business-to-business transactions. In November 2019, the Polish government provided a new provision under the Polish Penal Fiscal Code which sets out that a taxpayer who pays the total of an invoiced amount without the split payment mechanism, in contrast to their obligation, commits a fiscal offence.

In accordance with the guidelines of the Minister of Justice, prosecutors conducting investigations regarding VAT fraud should always consider extended confiscation and forfeiture of an enterprise. In cases involving extortion of more than 1 million zlotys, the Minister demands severe punishments of imprisonment.

When it comes to criminal liability for fiscal delinquency and crimes, at the end of 2019, the penalty for fiscal delinquency increased to between 260 and 52,000 zlotys. The maximum fine for fiscal crime increased to 24,960,960 zlotys.

In November 2019, the new amendment of the Act on Money Laundering and the Prevention of Financing Terrorism came into force. The revision was to implement the provisions of Directive 2015/849 of the European Parliament and of the Council. One of the most important changes put the obligation on beneficial owners or partners (including shareholders) of institutions obliged to report on specific transactions to have no criminal record of an intentional criminal offence or an intentional fiscal offence. Moreover, if it is found that an obliged institution has infringed particular obligations referred to under the Act, the legal authorities may impose financial penalties also on the members of the management body or other individuals responsible for the infringement.

Another important amendment is the revision of the Code of Criminal Procedure in October 2019. The main purpose of the revision is to speed up and simplify criminal proceedings at the judicial stage. However, the amendments undermine some procedural guarantees of the accused. For instance, the revision provides for the statute of repose to limit the time within which the parties are entitled to report the evidence. Other crucial changes
include the possibility of conviction by the court of appeal after a conditional discontinuance of proceedings in the first instance or the possibility for the court of appeal to make the sentence more severe by imposing a life imprisonment sentence. On the other hand, in a case in which no public prosecution counsel participates, the failure of the subsidiary prosecutor and their attorney to appear at the main trial without justification shall be deemed to be withdrawal of the charge.

These amendments lead to the conclusion that parties to criminal proceedings will be forced to involve a professional attorney in any case.

In January 2019, the Polish government published the last Draft of the Act on Liability of Collective Entities for Acts Prohibited under Penalty. The key purpose of the new Act was to enhance the effectiveness of preventing and fighting serious economic and tax crime, including corruption. The effective tools included, inter alia, more extensive liability, new obligations imposed on collective entities (such as the obligations regarding whistle-blowers, compliance and internal issues) and stricter sanctions. The most important changes included were: (1) no closed list of criminal offences the liability for which may be incurred by collective entities; and (2) the possibility to hold a collective entity liable without the natural person having been previously convicted by a valid court judgment.

This amendment was to introduce severe penalties and other sanctions. The proposed penalties were a fine of 30,000 zlotys to 30 million zlotys (in special cases, 60 million zlotys); and the dissolution or liquidation of the collective entity. The works on the Draft of the Act on Liability of Collective Entities for Acts Prohibited under Penalty were stopped in November 2019 at the end of the parliament’s previous term.

Another legislative tendency that occurred in 2019 relates to the matter of whistle-blowing. As was already mentioned, Poland has provided an obligation on any legal entity that issues or proposes to issue securities to have procedures for anonymous employee reporting. What is more, Poland must implement Directive 2019/1937 of the European Parliament and of the Council on the protection of persons reporting on breaches of EU law by 17 December 2021, which includes plenty of requirements regarding whistle-blowers. The new rules are going to be applied very widely. Pursuant to the provisions of the Directive, all enterprises having 50 or more workers should be subject to the obligation to establish internal reporting channels, irrespective of the nature of their activities.

VI CONCLUSIONS AND OUTLOOK

The general outlook is that the government is ready to increase the effectiveness of preventing and combating serious economic and fiscal crimes, including corruption offences. This objective is to be achieved through increasing the scope of liability, imposing new obligations, introducing more severe sanctions and speeding up criminal procedures. For instance, the Ministry of Justice announced in May 2020 that it is working on new provisions on a preventive confiscation. The new law is supposed to consist of the possibility of taking over the assets (real estate, cars, money, etc.) which have belonged to a suspect accused of acting in an organised criminal group for the last five years. The Council for Entrepreneurship in Poland has opposed the idea of a preventive confiscation because of excessive interference with private property rights.

Notwithstanding the above, the year 2020 is going be different from any other year before because of the restrictions and limitations imposed by the Polish government to fight the covid-19 pandemic. In March 2020, the Polish courts limited the number of cases under
their review by cancelling the vast majority of public hearings during the pandemic. At the same time, law enforcement have also limited the actions they have taken. Hence, there is no doubt that the pandemic situation is going to have a big impact on the course of criminal investigations in 2020.
I INTRODUCTION

Corporate liability for criminal and regulatory offences has a long tradition in the Portuguese jurisdiction. In the past, Portuguese companies have become more concerned with proper corporate governance and more aware of the importance of effective and fully enforced compliance programmes, a fact that has led to an increasing relevance of internal mechanisms of control and supervision, as well as whistle-blowing channels and internal investigations.

According to Portuguese law, there are basically two types of possible offences: crimes and regulatory offences.

Crimes are investigated and prosecuted by an independent public prosecutor and judged in criminal courts. During the investigation stage, the Public Prosecutor’s Office will attempt to discover whether a crime was indeed committed, who were its agents, and to gather conclusive evidence of the existence (or not) of criminal liability. The Public Prosecutor’s Office is aided by a police force or, exceptionally, by an administrative authority (e.g., tax authorities in tax crimes, and the Portuguese Securities Market Commission in crimes against the securities market), to collect evidence of a possible criminal offence. However, some judicial diligences and acts must be ordered or authorised by a judge; namely, those acts or diligences that may affect fundamental rights.

During an investigation, a person against whom a criminal complaint is filed or who is a suspect will be named as the defendant and will have a privilege against self-incrimination; namely, the right to remain silent and also the right to request any measures to further the investigation. However, the public prosecutor is not obliged to pursue any of the measures requested except the defendant’s right to be heard.

At the conclusion of the investigation, the public prosecutor decides whether to indict the defendant or to dismiss the case.

In either an indictment or a dismissal, there is an optional stage in the criminal proceeding that is entirely conducted by a pre-trial judge. This optional stage is to decide whether the case should go to trial or not. A decision by the judge confirming the public prosecutor’s indictment cannot be appealed, and the trial will proceed.

Therefore, if there is an indictment by the public prosecutor or if a decision from the pre-trial judge finds sufficient evidence that the defendant has committed a crime, the case
goes to trial. This is the most important stage in criminal procedure, with full respect for the adversarial principle. At the end of the trial, the defendant will either be convicted or acquitted. It is possible, in certain circumstances, to appeal to a higher court the lower court’s decision.

Regulatory offences, on the other hand, are investigated and prosecuted by administrative entities, with varying degrees of independence. These entities or regulators can apply fines that are binding and enforceable unless the decision to apply the fine is contested in court by the defendant. Most regulatory offences, when appealed, are decided in criminal courts. However, regulatory offences can also be decided in administrative courts (e.g., tax offences and offences related to urban planning) or in a specialised court (e.g., competition, energy, and financial offences). Regulatory offences have, in general, more flexible substantive and procedural requirements and some legal frameworks index the applicable fine to a company’s turnover and establish collaboration and leniency programmes. These factors incentivise and reward internal investigations and self-reporting.

II CONDUCT

i Self-reporting

Under Portuguese law, there is no general duty to self-report. However, there are certain sectors, subject to supervision, where entities are required to report wrongdoing.

Specifically, the Portuguese Securities Code (Decree Law no. 486/99, of 13 November) requires financial intermediaries to report any facts that are connected to financial crimes. The Legal Framework of Credit Institutions and Financial Companies (Decree Law No. 298/92, of 31 December) establishes a similar duty, requiring the management and supervisory bodies of credit institutions to notify the Bank of Portugal of possible fraud, both internal and external, which may produce adverse effects on the institution’s results or capital. Failure to notify the authorities when required to do so is a regulatory offence.

In addition, self-reporting criminal or regulatory offences committed in a corporate context to authorities, as well as cooperating with authorities in general, allows a company to reap certain benefits, depending on the legal framework applicable to the offence in question.

Article 71, number 2, subparagraph e, of the Portuguese Criminal Code, establishes that an offender’s conduct after the fact is considered when fixing the applicable penalty, especially if that same conduct consists in repairing the consequences of the crime committed. In addition, the offender’s conduct after the fact may be used to assess whether the criminal procedure should be suspended under Article 281 of the Portuguese Criminal Procedure Code (one of the possible negotiated solutions under Portuguese Criminal Law).

The offender’s conduct after the fact is also relevant when fixing the applicable fine in various sectors of regulatory offence law, namely, under the Legal Framework of Credit Institutions and Financial Companies, the anti-money laundering legislation, the General Framework on Environmental Regulatory Offences and the General Framework on Regulatory Offences for the Media Sector.

Furthermore, certain laws establish specific regimes for self-reporting.

Under Article 405-A of the Securities Code, if the offender confesses and collaborates with the Portuguese Securities Market Commission on the collection of evidence, the applicable fine is lower, and its upper limits are halved.

Also, pursuant to Articles 75 through 82 of the Portuguese Competition Law, a company that self-reports a cartel or a concerted practice may benefit from leniency, which
may entail immunity from fines or the reduction of their amount. An amendment to the Portuguese Competition Law, which would transpose the ECN+ Directive, was proposed by the Portuguese Competition Authority to the government and is currently under discussion.

Articles 40 to 44 of the Framework on Regulatory Offences for the Energy Sector also establish a leniency programme like the one set out in Portuguese Competition Law.

**ii Internal investigations**

Internal investigations in a criminal context do not have a general framework in Portuguese jurisdiction.

However, internal investigations are not a common practice within the Portuguese jurisdiction to internally investigate the possible commitment of an offence, except in some specific areas, like labor law or competition law, where internal investigations are more common.

One of the reasons for the absence of more internal investigations in connection with possible criminal offences is probably the absence of plea bargaining in Portuguese criminal law and the strict limits within which a negotiated solution is allowed (there is no possible negotiated solution if the specific crime committed by the agent is punishable with imprisonment for more than five years). Because there are no plea bargains, there are significant limits to the effectiveness of internal investigations within the context of criminal liability and, therefore, companies do not feel encouraged to carry out those investigations.

However, when these investigations take place, there are different possible approaches, but they usually focus on analysing documents (on paper or digital documents) and on conducting interviews with some of the employees or members of the company.

Any internal investigation must follow the procedural guarantees set out in the Portuguese Labor Code, otherwise any sanctions applied against an employee may be invalid. Furthermore, under the General Data Protection Regulation, the Portuguese Personal Data Protection Law (Law No. 58/2019, of 8 August) and the Portuguese Safety in Cyberspace Law (Law No. 46/2018, of 13 August), all entities subject to their scope must implement adequate and appropriate measures to ensure the safety of stored data.

In the context of anti-money laundering legislation, namely Law No. 83/2017, of 18 August, obliged entities are required to examine and report activities that may be connected to possible money laundering or financing terrorism. Obliged entities must also record all filed complaints, and they must immediately proceed with the implementation of new due diligence measures whenever the complaint gives the obliged entity reasons to doubt the accuracy of the data provided by a client.

Internal investigations will most often start after someone within the structure reports facts or suspicions related to some possible wrongful activity inside the company. Usually, these investigations aim to identify the responsible party for the possible wrongful actions and therefore to protect the company from possible legal consequences, mainly criminal or regulatory. Therefore, the purpose of these investigations is to cooperate with the public authorities responsible for the investigation, providing some evidence or mitigating the company’s own liability.

Most legal scholars in Portugal believe that, to use the evidence collected in the internal investigation in the following legal procedure, it is important to assure that the rights foreseen in the legal procedure are also respected in the internal investigation. This means that there is a common concern not to convert internal investigations into pre-criminal or pre-regulatory procedures, benefiting from the absence of legal regulation on the matter. In this context,
some of the evidence collected in the internal investigation may not be allowed in the criminal procedure if it has been obtained without complying with the legal requirements, particularly those evidences that in a criminal procedure can only be obtained with a judge’s authorisation.

Once the company is named as a defendant, it has a privilege against self-incrimination. Therefore, the company has a right to remain silent, which means that the company’s legal representative has a right to refuse to answer questions and, within a criminal procedure, not to provide any evidence that may be used against the company in a criminal case.

However, in regulated activities, entities are bound to comply with a series of rules and duties. These duties may embody collaboration duties with the supervision authorities. These duties imply, essentially, the delivery of documents that certify whether the entity is complying with the rules of the sector. Therefore, within a supervision proceeding, performed by the supervisory authority of the relevant market or economic sector, entities may be obliged to deliver certain documents to those supervisory authorities (namely those documents that the entity is legally bound to prepare and maintain), even though those proceedings may end with an accusation and condemnation for a regulatory offence.

### iii Whistle-blowers

In Portugal, there is no general framework regarding whistle-blowing and the protection of whistle-blowers.

However, for certain sectors there is an obligation to develop internal mechanisms to protect whistle-blowing. For instance, the Portuguese Securities Code establishes that any person who has any knowledge of facts, information or evidence connected to possible wrongdoing shall report them to the Portuguese Securities Market Commission (Article 368-A et seq.). This Commission must protect the whistle-blower’s identity, except if a court decision rules that the Commission reveal the whistle-blower’s identity. The Portuguese Securities Code also establishes that if the report is true and in good faith, it cannot be deemed as possible ground for any disciplinary, criminal, civil or regulatory proceeding against the whistle-blower (Article 368-A, number 6).

Another example is the Legal Framework of Credit Institutions and Financial Companies (Decree Law No. 298/92, of 31 December) that establishes an obligation for credit institutions to develop specific, independent and adequate internal mechanisms to receive, handle and file any report on possible irregularities concerning the management, accounting organisation and internal auditing of the company (Article 116-AA). Those mechanisms must also protect the whistle-blower’s identity as well as his or her personal data and the reporting per se cannot be deemed as possible grounds for any disciplinary, criminal, civil or regulatory proceeding against the whistle-blower (Article 116-AA, number 2 and number 6).

Law no. 83/2017, of 18 August, also establishes that the obliged entities must create specific, independent and adequate internal mechanisms to receive, handle and file reporting on possible irregularities concerning anti-money laundering legislation (Article 20). Moreover, the obliged entities shall also protect the confidentiality of the whistle-blowing and the protection of the whistle-blower’s personal data (Article 20, number 2). The obliged entities shall not retaliate or discriminate against a whistle-blower and whistle-blowing per se cannot be deemed as possible grounds for any disciplinary, civil or criminal proceeding (Article 20, number 6).
A new version of the Portuguese Competition Law is currently being discussed and will most likely establish the protection of a whistle-blower who reports to the Portuguese Competition Authority any practice that may restrict competition.

In recent years, some companies have adopted internal measures to allow its members or employees to report possible offences in the company’s structure and to provide the possibility for whistle-blowers to assure their anonymity. The need to legally regulate this matter is a fact. It would be relevant to establish rules concerning the status of whistle-blowers and their protection against possible retaliation within the company’s structure.

Whistle-blowers may participate in criminal proceedings as a witness or even as a defendant and both have different legal status. A witness must answer every question truthfully during examination, while a defendant has a right to remain silent.

Although in the Portuguese jurisdiction there are no incentive programmes for whistle-blowing or specific rewards for whistle-blowers, if the whistle-blower reports some relevant facts or information to the competent public authorities, mainly to the Public Prosecutor’s Office, that conduct may help mitigate a penalty if the whistle-blower is a defendant in a criminal case and indicted by the public prosecutor. As mentioned above, Article 71 of the Portuguese Criminal Code establishes that, when determining a criminal fine, the court must consider the conduct of the defendant after the illegal fact, which may help whistle-blowers to mitigate their possible penalties by cooperating with the public authorities.

Although it is not designed to protect whistle-blowers, Law No. 93/99, of 14 July, establishes certain rules and programmes regarding the protection of witnesses. A witness may receive protection if his or her life, physical or psychological integrity, freedom, or material assets of high value are in danger because of the witness’ contribution to the case. This may help protect a whistle-blower’s identity and anonymity.

There is also the recent Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, on the protection of persons who report breaches of Union Law, as an EU instrument on whistle-blowing. Portugal has yet to bring into force the legislation and necessary provisions to comply with the final version of the directive.

III ENFORCEMENT

i Corporate liability

The rule in Portuguese criminal law is that only natural persons (individuals) are subject to criminal liability. However, the law establishes some exceptions, restricted to range of crimes, that allow extending criminal liability to legal persons (companies).

Article 11 of the Portuguese Criminal Code establishes that companies, except for the state or organisations acting within public authority, may be held liable for the crimes listed in paragraph 2, which include, among others: (1) trading of favours; (2) violation of prohibitions or restrictions; (3) bribery; (4) cronyism; (5) money laundering; (6) unlawful offering of an advantage; (7) corruption; and (8) embezzlement.

However, companies can only be held liable if a crime is committed on behalf of the company and for the company’s benefit or interest: (1) by an individual in a leadership position; or (2) by someone acting under the authority of an individual in a leadership position because of his or her lack of surveillance or control duties incumbent upon the latter.

An individual in a leadership position is a member of a governing body or someone who has the power to control the activity of the company.
The main exception to this regime is established for the specific case of tax crimes, where a company is held liable for actions performed on its behalf and for the company's benefit or interest, by governing bodies and any representatives (Article 7 of Law No. 15/2001, of 5 July).

A company can exclude its liability by evidencing that an individual has acted against its concrete orders and instructions. Corporate liability does not exclude individual liability and does not depend on it.

Other crimes can be committed by companies as per specific legislation (for instance, Law No. 20/2008, of 21 April, regarding corruption in international trade and in the private sector, and Law No. 52/2003, of 22 August, regarding counter-terrorism).

Besides criminal liability, companies can also be held liable for regulatory offences. The legal requirements are similar to the ones mentioned above regarding criminal liability. The main difference is that, although the General Framework on Regulatory Offences (Decree Law No. 433/82, of 27 October) determines that companies should be held liable for the offences committed by their governing bodies (Article 7), most courts have broadly interpreted said principle to include in its scope actions performed by workers, members of the board or any representatives. Once again, if the company is able to demonstrate that an individual's actions are a result of a violation of express orders or instructions, its liability can be excluded.

Other specific legal frameworks, namely the energy sector, the securities market sector and the banking sector, have adopted the same criteria followed by case law regarding the General Framework for Regulatory Offences.

On the other hand, for instance, the Competition Legal Framework has adopted a similar provision to the one established in the Portuguese Criminal Code.

If there are no incompatible positions between the company and its members or employees, it is not strictly forbidden that both the company and the individuals are represented by the same counsel. Besides, if the company's defence strategy also includes the defence of its employees, a joint legal representation or, at least, a closely coordinated defence is advisable. In that case, there is no issue regarding a company's paying the individual's legal fees connected to the case.

However, if the company argues that the individual's actions were committed against its orders or instructions, the defence shall be separately conducted. In such case, any counsel who represents both parties will be acting under a professional conflict of interest. In this regard, Article 99, number 3, of the Code of Practice of the Portuguese Bar Association (Law No. 145/2015, of 9 September), establishes that a lawyer shall not represent two or more clients in the same matter or a related matter, if there is a conflict of interest between those clients. If that is the case, it is not advisable for the company to pay the individual's legal fees.

Companies may also be held civilly liable for the conduct of their employees. According to Article 500 of the Portuguese Civil Code, companies are strictly liable for all damages caused to third parties by an individual acting in its name (even if the damages are intentionally caused or against the company's orders or instructions). Nevertheless, companies have a right of recourse against said individual unless it is demonstrated that the company itself has contributed to those damages.
Penalties

Under Portuguese Criminal Law, there are two kinds of criminal penalty that may be imposed on companies: main penalties and ancillary penalties. Pursuant to Article 90-A of the Portuguese Criminal Code, companies may be punished by penalties of a fine or with a judicial winding-up order.

The winding-up shall only be ordered if the company was incorporated with the exclusive or predominant intention to commit crimes, or if it is being used, exclusively or predominantly, to commit those crimes by those who have a leadership position.

The concrete application of a criminal fine depends on the decision of the court. Under Article 90-B of the Portuguese Criminal Code, fines are determined in two steps: (1) establishing the number of days that compose the fine, which may never be less than 10 and that is determined in accordance with the gravity of the offence; and (2) defining the monetary value of each day in accordance with its economic and financial situation as well as any obligations to workers; in each case, the monetary value of each day shall correspond to an amount between €100 and €10,000.

In cases in which the rule of criminal law does not set a day-rate system, but solely a prison sentence, the corresponding penalty for a company will still be a fine, in which a month in prison will be equivalent to 10 days of fine.

If the applicable fine is not higher than 240 days, the court is entitled to condemn companies by a simple admonition, as set forth in Article 90-C of the Portuguese Criminal Code.

Under Article 90-D of the Portuguese Criminal Code, if the applicable fine is not more than 600 days, the court is entitled to replace it for a good behaviour bail, from €1,000 up to €1 million. This bail will be retained by the court for one to five years. If the company, in that period, commits the same crime, the bail reverts to the Portuguese State.

Furthermore, the Portuguese Criminal Code sets forth the following ancillary penalties:

- adopting necessary procedures to cease the unlawful behaviour;
- prohibition of exercising a certain activity, from three months up to five years, if the crime was committed within the scope of the company’s activity;
- prohibition of engaging in certain agreements;
- prohibition of the right to receive public grants or subsidies;
- closing down of the business, from three months up to five years, if the crime was committed within the scope of the company’s activity; and
- advertisement of the condemning decision.

In sectorial areas of criminal law, namely the Criminal Framework for Corruption in the International Trade and in the Private Sector (Law No. 20/2008, of 21 April) and the Anti-Money Laundering Legislation (Law No. 83/2017, of 18 August), the company will be punished with a fine according to Article 90-B of the Portuguese Criminal Code.

As foreseen in Criminal Law, under the General Framework for Regulatory Offence there are two kinds of regulatory penalties that may be applied to companies: main penalties and ancillary penalties. The main penalty applicable is also a fine.

Regarding companies’ concrete penalties, in some areas of Regulatory Offences, namely, inter alia, the Anti-Money Laundering Legislation and the Legal Framework of Credit Institutions and Financial Companies, the maximum limit of the fine is aggravated
up to the following amounts: (1) 10 per cent of the annual business turnover of the financial year before the condemning decision; or (2) the double of the amount obtained as a result of the offence.

Likewise, the Portuguese Securities Code sets forth, in Article 388, number 2, that the maximum limits of applicable penalty may be aggravated up to the following amounts: (1) 10 per cent of the annual business turnover according to the last consolidated accounts approved by the board of directors in the financial year before the condemning decision; or (2) the triple of the amount obtained as a result of the offence committed.

Moreover, pursuant to Article 68, numbers 3 and 4, of the Portuguese Competition Law, the amount of the fine shall not exceed 10 per cent of the annual business turnover of the financial year before the condemning decision.

The main ancillary penalties applicable to companies, under the General Framework for Regulatory Offences, are the following:

a. loss of the benefit obtained as a result of the offence;

b. prohibition of exercising activities that depend of any authorisation granted by administrative agencies or other administrative authorities/bodies;

c. prohibition of the right to receive public grants or subsidies;

d. prohibition of the right to enter into public agreements;

e. closing down business whose operations depend on an administrative business licence;

f. the suspension of administrative authorisations and licences; and

g. advertisement of the condemning decision.

These ancillary penalties shall only be applied in a limited period of time set forth in each sectorial legal framework. In general, Article 21, number 2, of the General Framework of Regulatory Offences establishes that the ancillary penalties, except for loss of benefit, shall not be applied for longer than up to two years.

In some cases, taking into consideration, inter alia, the ne bis in idem principle, companies may be held both criminally and regulatorily liable. If these offences are in a relation of consumption, the main penalty for the offence should be the one applicable to the crime, together with possible ancillary sanctions established to the regulatory offence. However, it is possible for the authorities to design the indictment as both offences (criminal and regulatory) being concurrent, and therefore requesting the application of the penalties and sanctions foreseen for both offences.

### iii Compliance programmes

The existence of a compliance programme may be an important defence tool when a company faces a criminal or regulatory proceeding related to a possible offence.

However, it is mandatory that a company’s compliance programme is not only approved but also fully enforced within the company’s structure, with express statements and specific orders or instructions. It is not enough that the compliance programme defines the internal policy of the company, with a description of the company’s values and mission. A compliance programme, to be effective or legally relevant, must establish specific guidelines concerning the company’s activities, services and internal proceedings and mechanisms, and clearly stating what is forbidden according to the company’s policy. It is not enough to have a programme only written on paper or with general recommendations.

In order to establish and define such a programme, it is important that the company conducts a very careful risk assessment, taking into consideration its activity, business sector
and the already adopted internal proceedings. That risk assessment should also analyse the country's main features and the features of the countries where the company has commercial activities or trade relationships. This due diligence should also identify people and services that may represent a higher risk of disrespecting the rules and internal proceedings. And that due diligence and risk assessment must always be carried out regarding a counterpart in a business or contract, before initiating a formal relationship with that other company.

When it is defined and approved, the programme should be presented and explained to all members and employees and always accessible to be read and consulted. And it is advisable that the company develops and maintains an internal compliance department, working closely with management and several departments. The compliance department and the compliance officer shall be responsible for establishing rules, improving the internal proceedings and mechanisms, and for the constant updating of the internal programmes and duties. The company may also request an external and independent auditor to analyse its compliance programmes and internal proceedings, therefore granting an additional note of adequacy and sufficiency for those programmes and proceedings.

It is also important to have internal training sessions to explain the programme to all members and workers within the company's structure. Some compliance programmes may also include a disciplinary system in case of its violation, as well as a system for protection of whistle-blowers, to assure and protect their anonymity and the confidentiality of the reported information.

The specific regulation and legal relevance of the compliance programmes depend on the sector of activity. Usually, companies operating in the financial and economic sector have been more regulated than the others, facing more legal obligations in this matter.

As explained before, according to Article 11, number 6, of the Portuguese Criminal Code, a company may not be held criminally liable if it is able to prove that the individual, who adopted a certain conduct or behaviour, acted against concrete orders or instructions from one who has the authority within the company.

An adequate and fully enforced compliance programme may therefore be used as an argument of defence to exclude the company's criminal liability.

The same rule applies to certain regulatory offences, namely in the context of the energy sector (Article 37, number 3, of Law No. 9/2013, 28 January), the banking sector (Article 203, number 2, of Decree Law No. 298/92, of 31 December) and also offences regarding anti-money laundering (Article 162, number 2, of Law No. 83/2017, of 18 August). In what concerns the securities market legal framework, the company may not be held liable if the individual acted against express, specific and individual orders or instructions provided to him, before committing the offence (Article 401, number 3, of Decree Law No. 486/99, of 13 November).

Even if the compliance programme does not exclude the company's liability, it may help mitigate the penalty. According to Article 71 of the Portuguese Criminal Code, which establishes the general rules regarding the relevant factors that help determine the penalty, it is mandatory to consider all circumstances that may be against or in favour of the defendant. A compliance programme may help mitigate the severity of the offence or it may be deemed as previous conduct that mitigates the severity of the offence.

The same applies to regulatory offences, as a fully approved and enforced compliance programme may help mitigate the severity of the offence and the company's fault, according to Article 18, number 1, of Decree Law No. 433/82, of 27 October.
iv Prosecution of individuals

As mentioned before, according to Article 11, number 7, of the Portuguese Criminal Code, a company's liability does not exclude an individual's liability and does not depend on it.

In most legal cases investigated and ruled in Portugal, companies and some of their individual employees were simultaneously considered liable or, at least, simultaneously investigated. The Portuguese model of corporate liability is not strictly an example of personal liability, meaning that it is grounded on the wrongdoing of specific individuals that represent the company. Therefore, it is important to identify the individuals or group of individuals who committed the offence (or omitted a required conduct) on behalf of the company and for the company's benefit or interest.

This is also the rule in regulatory offences, namely in offences set forth in the energy sector (Article 37, number 5, of Law No. 9/2013, of 28 January), in the banking sector (Article 204, number 1, of Decree Law No. 298/92, of 31 December) and in the securities market sector (Article 401, number 5, of Decree Law No. 486/99, of 13 November).

As mentioned above, if there is no conflict of interest between a company and its members or employees, they can be represented by the same counsel.

IV INTERNATIONAL

i Extraterritorial jurisdiction

Article 4 of the Portuguese Criminal Code establishes that Portuguese criminal law shall be applied to the offences committed: (1) in the Portuguese territory, regardless of the offender's nationality; and (2) in Portuguese ships or aircrafts, unless international treaties and conventions to which Portugal is a party provide otherwise.

However, Article 5 mentions several cases in which Portuguese criminal law is also applicable, even though the offence is committed abroad. They are mostly related with:

- certain types of crimes, such as crimes concerning counterfeiting of currency, debt security and sealed values; crimes against national independence and integrity; crimes against the Constitutional State; sexual crimes; kidnaping; slavery; female genital mutilation; forced marriage; human trafficking and crimes against nature; as long as the offender is found in Portugal and cannot be extradited; or with
- the nationality principle, considering that the offence is committed by or against a Portuguese person, if: (1) the offender is found in Portugal; (2) the offence is also punishable under the law of the state where it was practiced; and (3) it is possible to extradite for such crime, but extradition is not granted in that case.

As for companies, according to Article 5, number 1, subparagraph g of the Portuguese Criminal Code, Portuguese criminal law is applied when an offence is committed abroad by or against a company that has its registered office in Portugal.

In relation to crimes concerning corruption in the international trade and in private sector, the above-mentioned general rule provided by Article 4 is also applicable. Nevertheless, under the terms of Law No. 20/2008, of 21 April, Portuguese law shall also be applicable in case: (1) of active corruption affecting international trade, in connection to offences carried out by Portuguese or foreigners who are found in Portugal, regardless where the offences were committed; or (2) of active or passive corruption in the private sector, regardless of where
the offences were committed, when whoever promises, requests or accepts an advantage or promise is a national official or holder of a national political load or, being Portuguese, is an employee of an international organisation.

Specifically concerning terrorism, Law No. 52/2003, of 22 August, provides that, besides the general rule, Portuguese law is also applied to offences committed abroad in case: (1) they constitute a crime of terrorist organisations or terrorism; or (2) when they constitute crime of other terrorist organisations, international terrorism or terrorism financing, provided that the offender is found in Portugal and cannot be extradited or handed over in execution of a European arrest warrant.

Concerning drug trafficking (Decree Law No. 15/93, of 22 January), Portuguese criminal law is still applicable to offences committed outside the national territory when they are carried out: (1) by foreigners, provided that the offender is in Portugal and is not extradited; or (2) on board a ship against which Portugal has been authorised to take the measures provided for in Article 17 of the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988.

In what concerns regulatory offences, the general rule is the same as provided for criminal offences.

However, there are some exceptions to this general rule provided by specific regulatory regimes. For instance, in what concerns the Legal Framework of Credit Institutions and Financial Companies, besides the general rule, Portuguese law is also applicable to offences committed abroad by credit institutions or financial companies having their registered office in Portugal and operating there through branches or by providing services, as well as by individuals who represent those entities or are their shareholders. On the other hand, Article 2 of Competition Law establishes that Portuguese law is applied to the prohibited practices and concentration of undertakings which take place in Portuguese territory or whenever these practices have or may have an effect there, provided that international obligations assumed by the Portuguese state are met.

ii International cooperation
Portugal has ratified numerous international instruments – bilateral and multilateral – that simplify the cooperation between states.

Being part of the Community of Portuguese-Speaking Countries, Portugal also participates in several conventions that ease the cooperation between those countries. These conventions cover specific terms for extradition, mutual assistance in criminal matters, and transfer of sentenced persons.

Moreover, as a European Union Member State, Portugal has a closer cooperation with other Member States. For instance, Law No. 65/2003, of 23 August, which implemented the European Arrest Warrant, is of utmost importance in EU cooperation, by eliminating the use of extradition, so the proceedings are swifter and with shorter time limits, albeit the rights of defence are respected. Moreover, Law No. 88/2017, of 21 August, establishes a regime for the enforcement of a decision rendered by a judicial authority of an EU Member State in another Member State concerning specific investigatory measures, to obtain evidence. The exchange of data and information between EU Member States in the context of an investigation is also eased by Law No. 74/2009, of 12 August. On the other hand, Law No. 36/2015, of 4 May, provides a regime for the recognition and supervision of the enforcement of decisions on constriction measures as an alternative to pre-trial detention, as well as the surrender of a person between EU Member States in the event of non-compliance with the measures
imposed. Law No. 158/2015, of 17 September, is also of maximum importance once it is concerned with the recognition of judgments rendered in the EU context, establishing a legal regime for the transmission and enforcement of decisions in criminal matters imposing prison or other custodial measures for the purposes of enforcing those decisions in the European Union. Finally, worth noting is Law No. 88/2009, of 31 August, which provides the legal framework for the issuance and transmission by a competent court in criminal matters, of decisions on the confiscation of property, or other products of crime, in the context of criminal proceedings, concerning their recognition and enforcement in another EU Member State.

Alongside international and European instruments, multiple national instruments have been approved to ensure international cooperation. The International Judicial Cooperation Law in Criminal Matters (Law No. 144/99, of 31 August) is the most relevant instrument, because it establishes a comprehensive regime concerning extradition, transfer of criminal procedures, enforcement of criminal judgments, transfer of sentenced persons, supervision of conditionally sentenced or conditionally released offenders and mutual assistance in criminal matters.

In relation to extradition, Portugal has signed a large number of bilateral treaties. According to those treaties, the principle of reciprocity is the basic principle that provides the possibility of extradition, subject to certain exceptions. Also, as a matter of principle, Portugal does not extradite its own nationals. Besides, for Portugal to grant extradition it is necessary that the offence at stake is considered a crime both in Portugal and in the requesting state and that such offence is punishable with a minimum of one year of imprisonment.

Finally, the extradition request shall be refused if: (1) there are grounds to admit that such request is based on any form of discrimination or for political reasons; (2) the offender’s procedural guarantees are diminished because of any discriminatory factor; or (3) the offence at stake is punishable by death, irreversible injury or with life sentence in the requesting state, unless it ensures that such penalties will not be applied.

The Cybercrime Law (Law No. 109/2009, of 15 September) establishes some rules regarding international cooperation. Under the terms of that law, among other rules and measures, the criminal police assures that a contact point is permanently available to provide expert advice to other contact points and to preserve data, to collect evidence and to locate suspects in case of urgency.

### Local law considerations

Regarding bank secrecy, Portuguese authorities may refuse to provide information in the context of an international investigation grounded on Article 78 of Decree Law No. 298/92, of 31 December. However, Article 81 of the same Decree Law provides a comprehensive regime not only concerning cooperation with other EU Member States, but also in relation to non-EU Member States, on a reciprocity basis, within the scope of cooperation agreements, regarding the information required for supervision on an individual or consolidated basis of credit institutions having their registered office in Portugal and of similar institutions having their registered office in those countries.

As regard data privacy, recently approved Law No. 58/2019, of 8 August, which alongside Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, limits the possibility of exchanging information regarding personal data. In relation to third countries, pursuant to Article 22 of Law No. 58/2019, of 8 August, the transfer of data to non-EU Member States or international organisations, carried out in
compliance with legal obligations, by public entities in the exercise of authority powers, are deemed to be in the public interest for the purposes of Article 49, number 4, of Regulation (EU) 2016/679.

Finally, regarding letters rogatory, Article 232 of the Portuguese Procedural Criminal Code establishes that Portuguese authorities can refuse to comply with those letters if: (1) the requested judicial authority is not competent to perform the act; (2) the request concerns an act prohibited by law or if it violates the Portuguese public order; (3) the execution of the rogatory affects the sovereignty or security of the State; and (4) the act entails the execution of a foreign court decision subject to review and confirmation and the decision is not revised and confirmed.

V YEAR IN REVIEW

In recent years, there have been some high-profile cases where a company’s liability has been analysed.

For instance, in the E-toupeira case, the criminal liability of Benfica SAD (a Portuguese football club) was dropped, because the court ruled that the individual offender did not occupy a leadership position within the company and that the offence had not been committed on behalf of the company nor was it committed for its benefit or interest. The court also ruled that the company did not violate any surveillance or control duties, through someone occupying a position of leadership, pursuant to Article 11 of the Portuguese Criminal Code.

As previously mentioned, in the context of the European Union, a directive on the protection of persons who report breaches of Union law was enacted (the Directive). This Directive applies to persons who work for a public or private organisation or who are in contact with such organisation in the context of their work-related activities that report any breach of the Union law possibly harmful to the public interest. This Directive aims to protect whistle-blowers against any possible retaliation by setting up safe internal reporting channels. Portugal shall bring into force the necessary laws, regulations, and administrative provisions to comply with this Directive by 17 December 2021.

Furthermore, Portugal has been working on new anti-bribery legislation for several years, including the regulation of lobbying activity and alternatives to the criminalisation of unlawful enrichment. There was a draft law on that matter that was dismissed as unconstitutional by the Portuguese Constitutional Court.

Regarding the regulation of lobbying activity, the statute approved by the Portuguese parliament on this subject in July 2019 was vetoed by the Portuguese President for having some insufficiencies that have yet to be rectified. The discussion on the regulation of lobbying activity, namely in what concerns the rules of transparency applicable to private entities that carry out legitimate representation of interests before public entities, is expected to proceed during the following months.

Moreover, in the past year, Law No. 52/2019, of 31 July, introduced the exclusivity obligation in the exercise of public office and the obligation to present, in a single document to be accessible online, all the income and asset declarations issued by holders of political positions and high public offices. This declaration shall also include every act and activity that may lead to incompatibilities and impediments of the holder of political position or high public office. In addition, under the Organic Law No. 4/2019, of 13 September, the Entity
for Transparency of Holders of Political Positions and High Public Offices was officially created as the body responsible for monitoring and assessing the truthfulness of the income and asset declarations issued by public officers.

VI CONCLUSIONS AND OUTLOOK

In the near future, some major criminal and regulatory cases in Portugal will have relevant developments. In particular, there will be a pre-trial decision on the possible submission to trial of the case known as Operação Marquês, where a former Portuguese Prime Minister is accused, among others, of the crime of corruption by a political office holder. Furthermore, some relevant decisions are also expected regarding criminal and regulatory investigations in the resolution of BES, one of the biggest banks in the Portuguese financial system. This occurred in 2014, but the investigations are still ongoing.

From a different perspective, it is expected that the Public Prosecutor’s General Office and the regulatory authorities of the financial system will continue to tighten their supervision on operations that may reveal evidence of money laundering – a trend that started in 2017, with the new law on the prevention and prohibition of money laundering and a possible increase of money laundering cases.

Finally, since the Portuguese indicators on public perception of transparency and illicit practices within the state administration are still not favourable, the discussion about new measures to fight against corruption is likely to continue, and new forms of leniency practices and agreements will be implemented.
Chapter 20

SINGAPORE

Jason Chan, Lee Bik Wei, Vincent Leow and Daren Shiau

I INTRODUCTION

The standards of corporate governance have a major role in the maintenance of Singapore’s reputation as a secure and established financial and business centre. Singapore is ranked first in ‘Doing Business 2016’ by the World Bank Group and has been lauded for its high standards of corporate governance by the 2014 CG Watch, ranking first with Hong Kong.

A number of regulatory bodies in Singapore are empowered to investigate and prosecute corporate misconduct:

a The Monetary Authority of Singapore (MAS) acts as the central bank of Singapore. The MAS is responsible for regulating and supervising the financial services sector, administering the Securities and Futures Act (SFA) and conducting surveillance on financial stability. Pursuant to Part IX of the SFA, the MAS has powers to require the disclosure of information about securities and futures contracts, to require the production and inspection of companies’ books, to enter premises to carry out investigations and to examine witnesses. Effective from March 2015, the MAS and the Commercial Affairs Department (CAD) of the Singapore police force jointly investigate potential market misconduct offences such as insider trading and market manipulation under Part XII of the SFA.2

b The Singapore Exchange Limited (SGX) acts as a front-line regulator to promote a fair, orderly and transparent marketplace and a safe and efficient clearing system through monitoring the continuing compliance of the Singapore Exchange Securities Trading Limited (SGX-ST) Listing Manual (the Listing Manual) and the review of listings applications. Enforcement of compliance with the Listing Manual by listed companies is performed through investigations by the SGX, with appropriate sanctions imposed for breaches.

c The Accounting and Corporate Regulatory Authority acts as the regulator of business entities, public accountants and corporate service providers.

d The Competition and Consumer Commission of Singapore (CCCS) is tasked with administering and enforcing the provisions of the Competition Act, which promotes competition in the markets, and the Consumer Protection (Fair Trading) Act, which protects consumers against unfair trade practices. The CCCS’s key sectors of focus in 2019 were digital platforms, transport, hospitality, and administrative and support services. The CCCS will take action against anticompetitive agreements, abuse of dominant

---

1 Jason Chan, Lee Bik Wei, Vincent Leow and Daren Shiau are partners at Allen & Gledhill LLP.
positions, and mergers and acquisitions that substantially lessen competition. As at 31 March 2019, the CCCS had completed 67 investigations relating to anticompetitive agreements and abuse of dominant positions (including leniency applications) and reviewed 83 merger notifications. The CCCS has the power to require the production of specified documents or information, to enter premises without a warrant, and to enter and search premises with a warrant, if the CCCS has reasonable grounds for suspecting that the provisions of the Competition Act have been infringed. In respect of its consumer protection function, the Consumers Association of Singapore (CASE) and Singapore Tourism Board (STB) are the first points of contact for complaints by local consumers and tourists, respectively. However, where errant retailers continue to persist in unfair practices, the CASE and the STB may refer them to the CCCS, which has the power to gather evidence, file timely injunction applications with the Singapore courts, and enforce compliance with injunction orders issued by the courts, against such errant retailers. An example would be the CCCS’s successful application to the State Courts on 28 November 2019 to obtain an injunction against Fashion Interactive and its director, Mr Magaud to stop them from engaging in an unfair practice known as a ‘subscription trap’ on its shoes e-commerce website, myglamorous.sg.

The Singapore police force has wide investigative powers pursuant to Part IV of the Criminal Procedure Code (CPC). In the course of its investigations, the police may issue written orders to summon any person in Singapore to attend and assist in investigations, failing which a warrant may be issued to order the attendance of that person. The police may also order the production of or access to documents and other relevant evidence necessary or desirable to any investigation and may search or apply for a search warrant in the event of non-compliance. The CAD is the principal department of the Singapore police force that investigates white-collar commercial and financial crimes and has similar powers. In April 2017, the MAS and the CAD announced the launch of a government-industry partnership to strengthen Singapore’s capabilities in the fight against money laundering and terrorism financing.3

The Corrupt Practices Investigation Bureau (CPIB) operates with functional independence and is mandated to investigate corruption offences under the Prevention of Corruption Act (PCA) and other related offences. CPIB officers have wide investigative powers pursuant to the PCA and may exercise all those powers in relation to police investigations given by the CPC in the course of CPIB investigations. Additionally, CPIB officers may, with authorisation from the Public Prosecutor, investigate any financial account or safe deposit box in any bank.

The Financial and Technology Crime Division of the Attorney-General’s Chambers is responsible for the prosecution and appeals of white-collar and other commercial crimes, including corruption cases investigated by the CAD and the CPIB.

It is generally advisable for all businesses, corporate entities and individuals under investigation to cooperate fully with the authorities and provide full and frank disclosure of material information. This is in view of the legislation in place to secure cooperation with many of the above authorities. For example, it is an offence under the SFA to refuse or fail to appear

---

before the MAS and render assistance in investigations. Further, Chapters IX and X of the Penal Code specify further offences such as (1) failing to attend before, (2) failing to produce a document and (3) furnishing false information to any public servant.

II CONDUCT

i Self-reporting

Singapore’s legislative and regulatory corporate governance framework has shifted from a merit-based approach to a disclosure-based regime of supervision. Under a disclosure-based regime, market participants are provided with better information, thus allowing them greater choice and freedom to take calculated risks, which promotes a more dynamic market.

To be successful, a disclosure-based regime requires an effective and robust enforcement regime to ensure accurate disclosure of material information to maintain the confidence of market participants.

Companies listed on the SGX-ST are required to comply continuously with the Listing Manual. Pursuant to Rule 703 of the Manual, listed companies must announce any information known to it concerning itself, or any of its subsidiaries or associated companies, that is (1) necessary to avoid the establishment of a false market in the securities of the listed company, or (2) would be likely to materially affect the price or value of its securities. Under Section 203 of the SFA, a listed company must not intentionally, recklessly or negligently fail to notify the SGX of information that is required to be disclosed under the Listing Manual. A breach of Section 203 of the SFA is not a criminal offence unless the failure to notify, if the company withholds disclosure, is intentionally or recklessly in non-compliance with Rule 703 of the Listing Manual. Section 331 of the SFA provides that directors may be prosecuted in their personal capacity for acts of the company provided that the non-compliance was committed with the consent or connivance of, or could be attributable to any neglect on the part of, the directors.

The Listing Manual is complemented by the revised Code of Corporate Governance 2012 (the CG Code 2012), issued by the MAS. Although compliance with the CG Code 2012 is not mandatory, listed companies are required under the Listing Manual to describe in their annual reports their corporate governance practices with specific references to the principles of the CG Code 2012. If the company deviates from any guidelines of the CG Code 2012, the deviation must be disclosed, with an appropriate explanation. The CG Code 2012 is aimed at increasing accountability and transparency, and the amendments are related to matters such as director independence, board composition, multiple directorships, alternate directors and disclosure of remuneration. In February 2017, the MAS announced that it had formed a Corporate Governance Council (the Council) to review the CG Code 2012. The Council has been considering how the ‘comply-or-explain’ regime under the CG Code 2012 can be made more effective. This includes ‘improving the quality of companies’ disclosure of their CG practices and explanations for deviations’ from the CG Code 2012.

In relation to competition law, the CCCS has implemented a leniency programme to incentivise cartel members to come forward and inform the CCCS of the cartel activities. To encourage self-reporting, a company stands to benefit from total immunity from financial penalties or any disqualification from participation in government contracts.

---

In January 2018, the Corporate Governance Council released a consultation paper on its recommendations to revise the Code of Corporate Governance 2012.
penalties if the company is the ‘first in the door’ to provide the CCCS with evidence of the cartel activity before an investigation has commenced, and provided that the CCCS does not already have sufficient information to establish the existence of the alleged cartel activity.

The company must also satisfy the following general conditions:

a. it provides the CCCS with all the information, documents and evidence available to it regarding the cartel activity;

b. it grants an appropriate waiver of confidentiality to the CCCS in respect of any jurisdiction where the applicant has also applied for leniency or any other regulatory authority it has informed of the conduct;

c. it unconditionally admits to the conduct for which leniency is sought and details the extent to which this had an impact in Singapore by preventing, restricting or distorting competition in Singapore;

d. it maintains continuous and complete cooperation throughout the investigation and until the conclusion of any action by the CCCS arising as a result of the investigation;

e. it refrains from further participation in the cartel activity from the time of disclosure of the cartel activity to the CCCS (except as may be directed by the CCCS);

f. it must not have been the one to initiate the cartel; and

g. it must not have taken any steps to coerce another undertaking to take part in the cartel activity.

In this regard, two companies (Koyo Singapore Bearing (Pte) Ltd and DHL Global Forwarding) have avoided financial penalties for their involvement in international cartel activities under the leniency programme. Full immunity was granted to both companies when they reported on price fixing to the CCCS.

If the company is not the first-in-the-door leniency applicant but provides evidence before the CCCS issues a proposed infringement decision, the company may still be granted a reduction of up to 50 per cent of the financial penalty, if the general conditions in points a to e above are satisfied. In particular, the CCCS, in its revised Guidelines on Lenient Treatment for Undertakings coming forward with information on Cartel Activity 2016, had clarified that coercers and initiators of cartels may also apply for leniency and may qualify for up to 50 per cent discount of the financial penalty.

The CCCS has reportedly seen an increase in the number of leniency applications and has recently stated that antitrust enforcement remains a priority for the CCCS, with bid-rigging cases in the pipeline. As at 31 March 2019, the CCCS had received leniency applications in 24 cases.

Notwithstanding that there is no obligation on retailers for self-reporting, retailers are nevertheless encouraged to work with the CASE, the STB and the CCCS to address complaints by local consumers and tourists.

ii Internal investigations

Generally, internal investigations are those that a company decides to carry out in relation to itself and into its own affairs. They may be prompted by regulatory concerns, or complaints from third parties, or concerns raised as a result of inquiries by independent directors and shareholders.

Internal investigations usually involve conducting interviews with employees, managers and directors, and the collection and review of hard-copy documents and electronic files stored on various forms of media (e.g., emails, telephone records or other electronic
transmissions). The involvement of external parties, such as lawyers, forensic accountants, private investigators or computer experts, may occasionally be required. During the course of its investigations, the company may be obliged to comply with its legal disclosure obligations (e.g., under the Listing Manual) and legal professional advice should be sought in this regard.

Depending on the seriousness and nature of the matter, the individuals being investigated may retain their own lawyers. If there are reasonable grounds to suspect that the investigations may lead to prosecutions, it is advisable to consider retaining lawyers at an early stage so that any statements given during the internal investigations that may be subsequently turned over to the police are given with the benefit of legal advice.

On the issue of maintaining legal professional privilege during an internal investigation, the Court of Appeal considered the doctrine of legal professional privilege in light of significant developments at common law in the case of *Skandinaviska Enskilda Banken AB (Publ), Singapore Branch v. Asia Pacific Breweries (Singapore) Pte Ltd*. The issue before the Court of Appeal was whether draft reports prepared and produced by an external accounting firm (and law firm) in respect of an internal investigation of Asia Pacific Breweries (Singapore) Pte Ltd’s (APBS) internal control systems and procedures attracted both legal advice and litigation privilege. The internal investigation by APBS was prompted by a fraud perpetrated by an APBS finance manager, who had obtained credit and loan facilities from banks. The action was brought against APBS to recover the monies after the fraud was uncovered. In the action, the banks sought specific discovery of the draft report.

On the issue of legal advice privilege, the Court of Appeal endorsed the decision of the Australian Federal Court in *Pratt Holdings Pty Ltd v. Commissioner of Taxation*, which held that whether privilege is accorded to documentary communications of a third party is dependent on the nature of the function the third party performed for the party that engaged it. Privilege will be accorded if the function was to enable the engaging party to obtain legal advice if required. This is as opposed to the nature of the relationship of the third party’s legal relationship with the party that engaged it. The Court of Appeal stated that ‘the approach taken in *Pratt Holdings* is principled, logically coherent and yet practical and is also consistent with the reality of legal practice’ and held that third-party communications could be covered by legal advice privilege, but it had to be demonstrated that the communications were made for the dominant purpose of obtaining legal advice.

On litigation privilege, the Court of Appeal set out the basic principles or requirements of litigation privilege as set out in Section 131 of the Evidence Act (i.e., if the dominant purpose for which the legal advice had been sought and obtained was for the anticipation or contemplation of litigation, the advice concerned would be protected by litigation privilege). The Court of Appeal held that as litigation was ‘foremost in the mind’ of APBS and the dominant purpose of the draft reports was in aid of litigation at the time, litigation privilege applied to the draft reports.

The Evidence Act was amended in 2012 to extend legal advice privilege to communications with in-house legal counsel for the dominant purpose of seeking legal advice.

Note that there are statutory exceptions to situations in which legal advice privilege may be asserted over communications or documents. In particular, Section 128(2) of the Evidence Act expressly states that ‘any communications made in furtherance of any illegal purpose’ or where ‘any fact observed by any legal counsel in an entity in the course of his [or her] employment as such showing that any crime or fraud has been committed since the commencement of his [or her] employment’ are examples of such exceptions.
In respect of litigation privilege, the High Court held in *Gelatissimo Ventures (S) Pte Ltd & Ors v. Singapore Flyer Pte Ltd* that litigation privilege under Section 131 of the Evidence Act is subject to the same fraud exception as found in Section 128(2)(b) of the Evidence Act. This is despite the literal wording of Section 131 of the Evidence Act, which suggests that litigation privilege is an absolute privilege.

### iii Whistle-blowers

Although there is currently no general overarching legislation in Singapore specifically addressing whistle-blowing, certain programmes and specific legislation have been created or enacted that address this issue. An example is the implementation of the CCCS’s leniency programme. The CCCS encourages businesses that are part of a cartel agreement or concerted practice, or a member of the general public who is aware of a cartel activity, to blow the whistle and provide information on cartel activity, and the CCCS will keep the identity of whistle-blowers confidential. In appropriate circumstances, the CCCS may also pay a monetary reward to informants for information that leads to infringement decisions against cartel members.

According to a press release by the CPIB, it received 808 complaints in 2016 (an 8 per cent decrease from the 877 complaints received in 2015), of which 118 were registered for investigation, as compared with 132 cases registered in 2015.\(^5\) In January 2017, as part of the CPIB’s anti-corruption efforts, the new Corruption Reporting and Heritage Centre (CRHC) began operations. The CRHC was set up to enable people to make complaints discreetly and in a more accessible manner. The identity of informants is protected under Section 36 of the PCA, which includes provisions that a complaint about an offence under the PCA shall not be admitted in any civil or criminal proceedings and no witness is obliged or permitted to disclose the name or address of any informer. The court is further obliged to redact or expunge any references to the name or identity of the informer that may be found in any document in evidence to protect the informer from discovery. Citing Section 36 of the PCA, the court has observed, in *Dorsey James Michael v. World Sport Group Pte Ltd*, that there is a compelling public interest consideration ever present in Singapore to encourage whistle-blowing against corruption.

The MAS has stated that supervision can only go so far in preventing corporate misconduct in the financial industry, and that the creation of a safe environment for whistle-blowing is necessary to build a culture of trust and strong values in the financial industry. In this regard, Guideline 12.7 of the CG Code 2012 provides that a company’s audit committee ‘should review the policy and arrangements by which staff of the company and any other persons may, in confidence, raise concerns about possible improprieties in matters of financial reporting or other matters’, and the ‘existence of a whistle-blowing policy should be disclosed in the company’s Annual Report, and procedures for raising such concerns should be publicly disclosed as appropriate’. Further, the Guidebook for Audit Committees (revised on 19 August 2014) lays out guidelines on the implementation, conduct and review of whistle-blowing policies within companies. The guidelines for whistle-blowing policies recommend the protection of the identity of the whistle-blower, and provide for independence, objectivity and fairness of the investigation and resolution process.

---

Courts take a dim view of whistle-blowers who knowingly provide false information. In *PP v. Mohd Ghalib s/o Sadruddin*, the court imposed a deterrent sentence of six months’ imprisonment against the accused for providing false information in a complaint to the CPIB. The court stated that the sentence was meted out as the correct signal must be sent so that like-minded individuals will think twice about blatantly lying about alleged conduct. Note that the court took pains to emphasise that the decision should not apply to whistle-blowing ‘done in good faith, which is a helpful check and balance, and there should not be a chilling effect on such conduct’.

### III ENFORCEMENT

#### i Corporate liability

In Singapore, corporate conduct is capable of attracting both criminal and civil liability. A ‘person’ is defined in law as including a body corporate unless a contrary intention arises. Hence, whenever a statute purports to impose liability on any person, a company can be held directly liable unless otherwise specified, or unless such a construction is inconsistent with the subject or context of the said statute.

**Concurrent liability of officers and employees**

Since a company is a legal construct, it has to act through its officers and employees; therefore, situations giving rise to a finding of corporate wrongdoing are likely to also involve wrongful conduct on the part of particular individuals.

In such situations, the potential criminal and civil liability of the company and these individuals are distinct and independent. That said, there is no bar against criminal or civil liability being imposed on both the company and these individuals concurrently, save for the prohibition against double recovery in the civil context.

**Criminal liability for conduct of officers and employees**

A company can be subject to criminal liability for the conduct of its officers and employees in one of several ways.

First, a company may be guilty of a strict liability offence; namely, an offence that does not require proof of a culpable mental state, such as intention, recklessness or knowledge. If a company’s officers or employees have caused the commission of a strict liability offence, the company may be held liable.

Second, a company may be guilty of being an accessory to the criminal conduct of its officers and employees. Accessory liability offences generally take the form of abetment or criminal conspiracy, and typically require some proof that the company was complicit in the conduct of its officers and employees.

Third, a company may be guilty of an offence if the criminal statute in question expressly makes a company liable for the acts of its officers and employees.

Fourth, and as a general catch-all, a company may be guilty of any other offence insofar as it is committed by the company’s organs (board of directors, or shareholders in general meeting) or agents. Under Singapore law, the acts of such organs and agents are regarded as the acts of the company.

A particular complication arises whenever an offence requires proof of a mental state because a company, by its very nature, has no ‘mind’ to speak of. In this regard, the matter is straightforward if the statute specifies how such a mental state is to be determined. Where
the statute does not, Singapore law recognises two methods of attributing the mental state of officers and employees to that of the company. First, the mental state of agents may be attributed subject to certain conditions. Second, the mental state of an officer or employee or such group of the same who is considered the ‘directing mind and will’ of the company may be attributed to that of the company (this would typically include directors or senior officers of the company).

**Civil liability for conduct of officers and employees**

A company can be subject to civil liability for the conduct of its officers and employees and is not exempt from any category of civil wrongs (e.g., contract, tort or equity). A company may be personally liable for the conduct of its agents and organs and may be vicariously liable for the tortious conduct of its employees insofar as the conduct was committed during the course of employment.

**Legal representation of a company and its officers and employees**

There is generally no objection to a company and its officers and employees being represented by the same counsel in the same matter where their interests are aligned. However, if a conflict or a risk of conflict between the interests of the company and the interests of the officers and employees exist, it is preferable that separate representation be sought to avoid the need for counsel to discharge him or herself from acting for both the company and the officers and employees.

**ii Penalties**

Save for custodial sentences, companies may generally be subject to the same penalties as natural persons (e.g., fines). That said, the corporate penal regime has several unique additional features.

First, companies may be subject to heightened criminal sanctions. Although the typical criminal sanction is the imposition of a fine, some statutes impose higher fine limits for companies.

Second, companies may be subject to regulatory sanctions on top of criminal sanctions. For instance, companies who hold regulatory licences may have their licences revoked under the terms of the licence or the authorising statutes under which the licences were issued. Also, if the company in question is listed on the Singapore Exchange, the Exchange is empowered to impose sanctions on the company for breaches of the Listing Manual. Such sanctions could include a private warning, public reprimand, suspension of the trading of its securities, or even delisting of the company.\(^6\)

Third, companies may avail themselves of deferred prosecution agreements (DPA) in certain situations.\(^7\) A DPA is a type of plea bargain. Under these agreements, prosecutors agree not to bring charges against a company in exchange for the company’s fulfilment of certain conditions within a fixed duration. Such conditions are not limited and may include cooperation in investigations, implementation of compliance programmes, and payment of financial penalties or compensation. The DPA option is only applicable to certain scheduled offences, including certain offences under the Corruption, Drug Trafficking and Other

---

\(^6\) See Rule 1417 of the Listing Manual.

\(^7\) See Part VIIA of the Criminal Procedure Code.
Serious Crimes (Confiscation of Benefits) Act (CDSA), the PCA and the SFA. All DPAs need to be approved by the High Court. After approval, the company will be deemed to be granted a discharge not amounting to an acquittal. Upon the expiry of the DPA and subject to the company’s compliance with the terms of the DPA, the High Court may, on the application of the Public Prosecutor, grant a discharge amounting to an acquittal.

iii Compliance programmes

Unless specifically provided for under a particular statute, the existence of a compliance programme does not generally function as a legal defence. That said, it is prudent for companies to institute reasonable internal compliance programmes depending on the risks that they foresee and the costs involved.

From the outset, the existence of compliance programmes may play a preventive function in that it may lower the risk of wrongdoing or, if any wrongdoing has already been committed, the duration of such wrongdoing (which may affect any penalties imposed on the company subsequently).

Compliance programmes may also be relevant at one of three stages insofar as criminal proceedings are concerned. First, prosecutors may take into account the existence of a compliance programme when exercising their discretion to prosecute. Second, DPAs may be conditioned on the institution of compliance programmes or the implementation of changes to existing compliance programmes. Third, the existence of a compliance programme may be relevant after the conviction of a company, as a mitigating factor during sentencing.

Beyond the company, compliance programmes may also assist the officers and employees of a company insofar as their personal liabilities are concerned. Such programmes may allow the officers and employees to show that any offence that they are accused of was not committed as a result of their consent, connivance or neglect.

iv Prosecution of individuals

Where there has been corporate wrongdoing, there is no bar prohibiting the authorities from holding a particular individual liable under criminal law as well, whether in addition to liability on the part of the company or otherwise.

Further, if an officer of a company, especially a senior officer, is accused of corporate wrongdoing, this will likely have reputational effects on the company, regardless of whether the company itself is also charged. How the company manages the continued relations with the officer in question should, therefore, take such considerations into account.

There is no obligation on the part of the company to dismiss or discipline an officer or employee who has been the subject of a criminal investigation or charged with a criminal offence. That said, this is likely to be dependent on the company’s internal policies and the view that the company takes with respect to the individual’s conduct. In practice, most companies would have in place their own disciplinary or investigation procedures, which may apply where there have been allegations of wrongdoing against a particular employee. This is likely to be governed by the relevant employment agreement between the company and the employee.

Needless to say, companies should cooperate with investigators insofar as they are legally obliged to do so. For example, authorities may require that a company produces documents or information relevant to their investigations or require that witnesses (such as other employees of the company) attend to be examined.
There is no bar against the company coordinating with the individual’s counsel. This may be a course that the company may wish to take where the interests of the company and the individual are aligned. There is also no legal bar against the company paying for the legal fees of the employee. In practice, it is common for a company to purchase directors’ and officers’ insurance, which may indemnify the legal costs to be incurred by an individual director or officer who is subject to criminal allegations. How such policies may operate, including the scope and extent of coverage, would depend on their precise terms.

IV INTERNATIONAL

i Extraterritorial jurisdiction

There is generally a presumption against the extraterritorial application of Singapore criminal statutes. That said, specific statutes have been enacted by Parliament to extend the reach of particular criminal laws beyond Singapore’s borders. Some key examples are discussed below.

Prevention of Corruption Act

The PCA, which is the principal anti-bribery statute in Singapore, expressly provides that it would apply extraterritorially to Singapore citizens outside Singapore. Section 37(1) of the PCA states:

The provisions of this Act have effect, in relation to citizens of Singapore, outside as well as within Singapore; and where an offence under this Act is committed by a citizen of Singapore in any place outside Singapore, he may be dealt with in respect of that offence as if it had been committed within Singapore.

Therefore, if a Singapore citizen commits an offence within the meaning of the PCA outside Singapore, he or she would be held liable as though it was committed within the Singapore territory.

Terrorism (Suppression of Financing) Act

The Terrorism (Suppression of Financing) Act, which is one of the key pieces of anti-terrorism financing legislation in Singapore, also contemplates extraterritorial application. It provides at Section 34 that certain offences committed outside Singapore would be deemed to be committed in Singapore and that the person in question may be charged, tried and punished accordingly. In addition, it also provides that if a Singapore citizen commits certain other offences outside Singapore, he or she may be dealt with as though the offence was committed in Singapore.

Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act

The CDSA, which is the principal statute criminalising money laundering, also contemplates extraterritorial application. This is clear from Sections 3(1), 3(3) and 3(5) of the CDSA, which respectively state that the Act ‘shall apply to any drug dealing offence or foreign drug dealing offence’, ‘shall apply to any serious offence or foreign serious offence’ and ‘shall apply to any property, whether it is situated in Singapore or elsewhere’. This is also evident from Section 2(1), which defines ‘criminal conduct’ and ‘drug dealing’ as the doing of such acts ‘whether in Singapore or elsewhere’.
Organised Crime Act 2015

Finally, the Organised Crime Act 2015 contains provisions that are intended to prevent and disrupt the activities of both local and transnational criminal organisations. To this end, the definition of ‘organised criminal group’ under Section 2 includes groups ‘based within or outside Singapore’ whose purposes include obtaining material benefit from the commission or facilitation of ‘any act outside Singapore that, if it occurred in Singapore, would constitute [a] serious offence’ as defined under the Act.

International cooperation

Mutual Assistance in Criminal Matters Act

The Mutual Assistance in Criminal Matters Act (MACMA) sets out the framework for mutual legal assistance between Singapore and other states in criminal matters. It allows the Singapore authorities to provide assistance to other states in respect of criminal investigations or proceedings concerning certain offences, without the need for a mutual legal assistance treaty between the requesting state and Singapore, on the basis of reciprocity.

The assistance Singapore may provide to other states in respect of criminal matters under the MACMA includes:

- taking of evidence;
- production of things (including documents);
- securing the attendance of a person;
- securing the custody of a person in transit;
- enforcement of a foreign confiscation order;
- search and seizure;
- locating or identifying persons; and
- service of process.

The Attorney-General’s Chambers handled 1,159 mutual legal assistance and extradition matters in 2018, compared with 957 in 2017.

Extradition Act

Extradition is possible and not uncommon in Singapore. The Extradition Act (EA) is the primary statute that governs the extradition of fugitives to and from foreign countries and territories. It sets out a general regime in respect of ‘foreign State[s] . . . between which and Singapore an extradition treaty is in force’ and 40 ‘declared Commonwealth countries’. Additionally, it also contains a set of specific rules that are only applicable to extradition to and from Malaysia (Part V of the EA).

Under the general regime, extradition out of Singapore is only allowed in respect of persons who are accused of or have been convicted of committing an ‘extradition crime’ within the defined meaning of the EA.

In the case of a foreign state, this refers to an offence against the law, or part of the law, of the foreign state; where the act or omission constituting the offence would, if it took place in Singapore, constitute an ‘extradition crime’ within the defined meaning of the EA.

---

9 Attorney-General’s Chambers’ Annual Summaries 2017, page 42.
10 See Section 2(1) of the EA.
place in Singapore, constitute a Singapore law offence described in the First Schedule to the EA (or would be so described if the relevant description contained a reference to the necessary state of mind or circumstance of aggravation).

b In the case of a declared Commonwealth country, this refers to an offence against the law, or part of the law, of the declared Commonwealth country that is punishable with a maximum penalty of death or imprisonment for not less than 12 months; where the act or omission constituting the offence would, if it took place in Singapore, constitute a Singapore law offence described in the First Schedule to the EA (or would be so described if the relevant description contained a reference to the necessary state of mind or circumstance of aggravation).

Embodyed in the definition of an ‘extradition crime’ is the requirement of double criminality. In considering whether the requirement of double criminality is satisfied, the Singapore courts will apply what is known as the ‘conduct test’, which requires that the conduct forming the basis of the relevant offence be punishable in both the extraditing state and the requesting state. The Singapore courts will not apply the ‘ingredients test’, which requires strict correspondence or identity between the elements of the foreign offence and the elements of the local offence.

**Informal cooperation**

In addition to the above, various Singapore agencies are also parties to informal channels of cooperation with agencies of other countries. For instance:

a The MAS is a signatory to a number of bilateral and multilateral memoranda of understanding (MOUs) that establish arrangements for, among others, information sharing and mutual assistance in regulatory actions.

b The Singapore police force (SPF) is a member of Interpol. Additionally, under the CDSA, the SPF’s Suspicious Transaction Reporting Office (STRO) is authorised to share information with foreign financial intelligence units (FIUs) subject to certain conditions.11

c Other Singapore agencies, such as the CPIB and the Central Narcotics Bureau, have their own informal bilateral relationships with their counterparts in other jurisdictions.

Singapore is also a member of the Financial Action Task Force (FATF), a 39-member intergovernmental standards-setting body that develops and issues guidelines on combating international money laundering and terrorism financing. The Ministry of Home Affairs, the Ministry of Finance, and the MAS jointly lead Singapore’s inter-agency effort to implement and maintain legislative and regulatory compliance with periodic FATF recommendations.

**iii Local law considerations**

Singapore has certain laws that may impose limitations on the sharing of information across jurisdictions. For example:

---

11 See Section 41 of the CDSA.
Banking secrecy laws prohibit licensed banks from disclosing customer information that would include, but is not limited to, any information relating to an account of a customer of the bank or any information relating to any deposits of a customer of the bank.\(^\text{12}\)

Similarly, data privacy laws provide that any data that is collected by any organisation that can be used to identify an individual cannot be disclosed unless the individual gives or is deemed to have given his or her consent.\(^\text{13}\)

Additionally, before the STRO shares information with a foreign FIU under the CDSA, the foreign FIU needs to provide appropriate undertakings for protecting the confidentiality of information shared and controlling its use, including an undertaking that such information will not be used as evidence in any proceedings.\(^\text{14}\)

That being said, if a court order is obtained under the MACMA for the production of a thing or description of a thing for the purposes of foreign criminal matters, the MACMA provides for civil and criminal immunity to any person who acts in good faith to comply with the court order; hence, any production in compliance with the court order will not be treated as a breach of any restriction on disclosure (whether imposed by law, contract, or rules of professional conduct).\(^\text{15}\)

V  YEAR IN REVIEW

The past year has seen a continued focus on investigation and enforcement in relation to corporate misconduct in Singapore’s financial markets.

In August 2019, the MAS issued a consultation paper on ‘Requirements on Controls against Market Abuse’\(^\text{16}\). The consultation paper sought comments on proposals to improve controls and facilitate investigations into market abuse, including market manipulation and insider trading. The proposed requirements are intended to apply to licensed and exempt financial institutions in Singapore that undertake the regulated activity of dealing in capital markets products.

One of the proposed requirements in the consultation paper is for financial institutions to record all communications between their trading representatives and the person instructing the order and trade in the customer’s account, even if the communication does not result in an actual transaction. This will include communications such as instant messages on personal electronic devices.

In February 2020, the MAS also published a staff paper on cyber risk in the financial sector. This paper focused on Singapore as a case study, and discussed the impact that cyberattacks can cause to financial institutions, including solvency, liquidity, market, operational, legal and reputational risks.\(^\text{17}\) The paper concluded that cyber risk poses a

---

\(^{12}\) See Sections 40A and 47 of the Banking Act.

\(^{13}\) See Sections 2(1) and 13 of the Personal Data Protection Act 2012.

\(^{14}\) See Section 41(2) of the CDSA.

\(^{15}\) See Section 24 of the MACMA.


growing threat to financial stability, and many questions remain that will require further analysis. Public agencies will need to do more to better understand and assess its financial stability implications.

Transnational investigations have featured prominently in the CAD’s profile in the past year. The Singapore Police Force signed a Memorandum of Understanding with the Antwerp Police Department in 2019, to enhance cooperation in information sharing, capability building and training. In 2019, the CAD announced that a transnational internet love scam syndicate based in Malaysia had been crippled through the joint efforts of enforcement agencies in Malaysia, Hong Kong, Macau and Singapore. In 2020, the CAD announced that a transnational fraud syndicate based in Malaysia had also been crippled through the joint efforts of the Singapore Police Force and Royal Malaysia Police. The Singapore Police Force has also focused its attention on scams involving the impersonation of local and foreign government officials.

More corruption-related reports were investigated by the CPIB in 2019. The vast majority (90%) of corruption-related reports concerned private sector cases. Public sector corruption remains low in Singapore, which was ranked fourth in the Transparency International Corruption Perceptions Index for 2019.

VI CONCLUSIONS AND OUTLOOK

Since the start of 2020, Singapore’s enforcement authorities have increasingly been dealing with cases of misconduct arising from the global covid-19 pandemic. These have included government official impersonation scams, business collapses and fraudulent scams involving government subsidy payments. This trend is expected to continue as fraudsters seek to exploit uncertain circumstances created by the pandemic.

The CAD had noted in its Annual Report that government subsidies meant to support businesses and defray rising health costs inadvertently open up areas for opportunistic fraudsters to exploit. Singapore’s enforcement authorities have made it clear that they will take a tough stance against criminals who seek to exploit such schemes. This is in line with Singapore’s consistent stance that it will spare no effort to safeguard Singapore’s status as an international financial hub, and the country’s reputation as a corruption-free business environment.

22 CAD Annual Report 2018, issued on 6 September 2019
SOUTH KOREA

Seong-Jin Choi, Tak-Kyun Hong and Kyle J Choi

I INTRODUCTION

The Prosecutors’ Office has the power to investigate and prosecute an individual or entity (including corporations) for almost all criminal offences. The police have the power to investigate general crimes such as fraud, embezzlement and forgery of documents. In addition, specific government agencies are granted the authority to investigate certain crimes: the National Tax Service (NTS) for tax violations, the Korea Fair Trade Commission (KFTC) for competition law violations, the Financial Supervisory Service (FSS) for securities-related crimes, the Ministry of Employment and Labour for labour law violations and the Ministry of the Environment for environmental law violations, among others. Under a new law to take effect on 15 July 2020, the High Public Official Investigation Agency will have the power to investigate and prosecute certain high-ranking public officials for certain crimes, such as corruption, and crimes related to their office.2

The police and the aforementioned government agencies are permitted to conduct dawn raids with the cooperation of the Prosecutors’ Office and with a court-issued warrant. Agencies such as the NTS and KFTC more often conduct on-site investigations and request voluntary production of documents and evidence; failure to cooperate with such a request can result in broader and more stringent investigations. As a practical matter, government investigations can be divided into two major categories: an investigation initiated by the relevant authority is termed a ‘special investigation’, while an investigation initiated with the filing of a criminal complaint by an aggrieved party is termed a ‘routine investigation’. Domestic political concerns often affect the prosecutorial function of special investigations but have less influence over routine investigations. The individual or entity being investigated in a routine investigation may take an adversarial stance; however, such a stance would be difficult to sustain in a special investigation because lack of cooperation frequently triggers investigations that are longer in duration, and broader and more stringent in terms of scope.

1 Seong-Jin Choi and Tak-Kyun Hong are partners and Kyle J Choi is a senior foreign attorney at Shin & Kim.
2 The Act on the Establishment and Management of High Public Officials Investigation Agency will take effect from 15 July 2020.
II CONDUCT

i Self-reporting

In general, there is no obligation for a business to self-report its misconduct. There are also no benefits enumerated in the laws or written policies for a business that self-reports its misconduct. Nonetheless, there may be incentives for a business to self-report. If the business in question is being subjected to a special investigation, the authorities may narrow the scope of the investigation, the number of charges or the entities to be indicted, or may close the investigation early, if the authorities determine that self-reporting has substantially assisted the investigation process. Any benefits are provided or negotiated on a case-by-case basis, rather than being prescribed in accordance with formal procedures. In terms of sentencing, self-reporting is a mitigating factor.

In cartel investigations, there is a written leniency policy for self-reporting; in fact, self-reporting has become a trend. A self-reporter, with some preconditions, may be eligible for mitigation of or exemption from administrative sanctions. To be eligible for exemption from administrative surcharges and restraining orders, the self-reporter must meet all the following requirements:

a the self-reporter must, voluntarily and independently, be the first person to provide evidence necessary to prove the existence of a cartel;

b the KFTC must have insufficient evidence to prove the cartel and must not have initiated the investigation;

c the self-reporter must remain cooperative until the investigation is complete; and

d the self-reporter must have suspended its collusive practice.

A business that provides the evidence necessary, regardless of whether the KFTC has initiated its investigation when self-reporting was conducted, to prove the existence of a cartel voluntarily and independently but second-in-order (i.e., another business has already self-reported) is eligible for a 50 per cent reduction of the administrative surcharge and mitigation of the restraining order, provided it remains cooperative until the investigation is complete and it has suspended its collusive practice.

---

3 However, certain financial institutions have obligations to report wrongdoing upon discovery (Article 12 of the Act on the Aggravated Punishment, etc. of Specific Economic Crimes). The rationale seems to be that certain financial institutions provide public functions.

4 ‘Circumstances after the commission of the crime’, which includes self-reporting, is one of the sentencing factors (Article 51.4 of the Criminal Act). Voluntary confession to the authorities by the representative of a corporation may exempt or mitigate criminal punishment (Article 52 of the Criminal Act, Supreme Court of Korea judgment, 95DO391, 25 July 1995). Self-reporting is a mitigating factor in the Sentencing Guidelines (http://sc.scourt.go.kr/sc/engsc/index.jsp).

5 Article 22.2 of the Monopoly Regulation and Fair Trade Act.

6 There are certain exceptions to this leniency. See Article 35 of the Enforcement Decree of the Monopoly Regulation and Fair Trade Act; ‘Public Notification on Implementation of Leniency Programme, Including Corrective Measures against Voluntary Confessors, etc. of Unfair Cartel Activities’ (Korea Fair Trade Commission (KFTC), Public Notification No. 2017-20, 14 November 2017).
ii Internal investigations

Generally, internal investigations are led by internal counsel, and the advisement from or representation by external counsel begins when a criminal or a civil complaint is filed against the wrongdoers. Therefore, it is relatively uncommon for an internal investigation to be conducted by external counsel.

Businesses have no obligation to share the results of an internal investigation with the government. Interviews with witnesses and examination of emails, documents or financial transactions are the typical means used during an internal investigation. Although there is no established law or practice regarding an employee’s retention of legal counsel during an internal investigation, employees tend not to retain their own counsel insofar as they are not in an adversarial position against their employer.

According to precedent set by the Supreme Court, attorney–client privilege or attorney work-product privilege for communications between an individual and his or her counsel is not recognized prior to the commencement of a criminal investigation or criminal proceedings. It is not clear whether the Supreme Court recognizes this privilege if communications are made after criminal proceedings have commenced. In any case, an attorney has a duty not to disclose confidential information and has the right: to refuse seizure of objects that come under his or her custody in the course of providing legal services and that are related to another’s confidential information; and to remain silent before the court on matters regarding confidential information. The aforementioned duties and rights are only afforded to attorneys. The client cannot assert these rights once he or she has been requested to produce such information. There have been a few incidents in which the Prosecutors’ Office has requested external legal counsel to submit materials produced by or exchanged between a client and its external legal counsel upon obtaining a search and seizure warrant from the court. Following these incidents, the South Korean legal industry has been making attempts to formally introduce attorney–client privilege into legislation.

iii Whistle-blowers

Although whistle-blower reports have always triggered a number of government investigations, they have not been very common to date. However, with an increase in incentive programmes and a shift in public attitude towards whistle-blowers, there has been a rise in the number of reports. The major statutes guaranteeing protection for whistle-blowers are as follows: the Protection of Public Interest Reporters Act (PPA), the Act on Protection of Specific Crime Informants and Article 84-2 of the Framework Act on National Taxes. There are more than 50 guidelines declared by government agencies regarding incentive programmes for whistle-blowers. This legislation provides for prohibition of retaliation against whistle-blowers, provisions of personal security, monetary compensation to whistle-blowers and formulas for the calculation of compensation.

The major incentive programmes set forth in the PPA are as follows:

7 Supreme Court of Korea, judgment 2009DO6788, 17 May 2012.
8 Article 317 of the Criminal Act.
9 Article 112 of the Criminal Procedure Act.
10 Article 149 of the Criminal Procedure Act.
11 Articles 13, 15 and 26 of the Protection of Public Interest Reporters Act (PPA).
a retaliation against or interference with whistle-blowing is prohibited;\textsuperscript{13}  
\begin{enumerate}
  \item if a whistle-blower is involved in a criminal violation with regard to the subject of reporting, mitigation or exemption of punishment may be provided;\textsuperscript{14}
  \item compensation is to be provided where whistle-blowing has led to a direct recovery of or increase in the revenue of the government or public institutions through the imposition of criminal or administrative sanctions on the business;\textsuperscript{15}
  \item a whistle-blower’s disclosure of confidential business information to the authorities is not deemed a violation of his or her employment agreement or any other laws or regulations;\textsuperscript{16}
  \item a business may not claim damages against a whistle-blower even if it suffers damage as a result of the whistle-blower’s reporting, unless the reporting was a false claim, the whistle-blower requested money or undue favour in the workplace in connection with the reporting, or the reporting was for other unlawful purposes;\textsuperscript{17} and
  \item the personal information of the whistle-blower may be treated on a no-name basis\textsuperscript{18}
\end{enumerate}

\section*{III ENFORCEMENT

\begin{enumerate}
  \item Corporate liability
\end{enumerate}

Although the Criminal Act, which traditionally covers most common types of crimes, does not recognise corporate criminal liability, various other statutes imposing industry-specific or subject-specific regulations (e.g., those on securities, construction, pharmaceuticals, public procurement, taxation, labour, competition, environment) usually recognise corporate criminal liability. The standard wording used in these statutes with respect to corporate criminal liability is that:

\begin{quote}
if a representative, agent, or employee of a corporation ('corporate representative') violates . . . [a provision in an Act] . . . in connection with the business of the corporation, the corporation itself, as well as the corporate representative, may be subject to . . . [a criminal fine] . . . provided that the foregoing shall not apply if the corporation was not neglectful in paying due attention to and supervising the relevant affairs, in order to prevent such violation.
\end{quote}

To assess whether the actions of an employee were committed in connection with the business of the corporation, all the circumstances should be taken into account, including:

\begin{enumerate}
  \item the scope of the corporation’s business;
  \item the title and position of the employee in question;
  \item the relevance between the illegal act committed by the employee and the business of the corporation;
  \item whether the corporation knew of the commission of the conduct or was involved therein; and
\end{enumerate}

\begin{footnotes}
\footnote{13} Article 15 of the PPA.
\footnote{14} Article 14 of the PPA.
\footnote{15} Article 26 of the PPA.
\footnote{16} Article 14 of the PPA.
\footnote{17} ibid.
\footnote{18} Article 12 of the PPA.
\end{footnotes}
the source of the money used in carrying out the conduct, and to whom the profit therefrom is attributed. 19

A Supreme Court case has held that the ‘employee of a corporation’ in the above provision shall include not only those who are formally employed by the corporation in question, but also those who directly or indirectly perform the duties for the corporation while under its direct control or supervision. 20

With respect to civil liability, the principle of respondeat superior applies. 21 The burden of proof is on the employer to prove that it has exercised due care in appointing the employee and in supervising the performance of the specific affair, or that the loss would have been inflicted even if the employer had exercised due care. 22

The Ethical Code of the Korean Bar Association prohibits representation of multiple clients in one case when there is any conflict of interest between them, unless all the clients consent and such representation does not prejudice any of the clients. 23 There is not a significant volume of court precedent on this issue, but it is not uncommon, at least during the investigation phase where the conflict between the corporation and the implicated individuals has not yet materialised, for a corporation and the implicated individuals to be represented by the same counsel.

ii Penalties
The punishable violations and the corresponding punishments and sanctions are stipulated in the relevant act; the most common punishments imposed on businesses are criminal fines and administrative surcharges. For certain violations, a restraining order or the revocation or suspension of a licence is imposed. In cases involving public procurement contracts, the sanction can be debarment; 24 the ceiling for the debarment period is two years. 25 Considering the stipulated range of sanctions and the practice of each government authority, administrative surcharges for violations of competition law are usually the most severe consequences, with the amounts often exceeding tens of billions of won. 26 So far, we have not seen other types of violations that frequently entail the enforcement of monetary sanctions of such magnitude. Various statutes provide for the revocation of corporate licences as a sanction for severe violations, and suspension of licences as a sanction for moderate violations. Generally, the period for licence suspension does not exceed three years and the suspension may be substituted by an administrative surcharge. These criminal or administrative sanctions are, depending on the underlying statutes, either mandatory or discretionary. Criminal sanctions are enforced by the Prosecutors’ Office. Administrative sanctions such as surcharge, restraining order, revocation or suspension of corporate licences, or debarment is enforced by the competent

19 Supreme Court of Korea, judgment 96DO2699, 14 February 1997.
20 Supreme Court of Korea, judgment 93DO344, 14 May 1993.
21 Article 756 of the Civil Act.
22 Supreme Court of Korea, judgment 97DA58538, 15 May 1998.
23 Article 22 of the Ethical Code of the Korean Bar Association.
24 Article 27 of the Act on Contracts to Which the State is a Party.
25 Article 27(1) of the Act on Contracts to Which the State is a Party.
26 In 2018, the number of cases in which the KFTC imposed an administrative surcharge was 181 and the total amount of surcharges imposed by the KFTC was 310.5 billion won (a simple calculation shows that 1.7 billion won was imposed per case). In 2017, the number of cases was 149 and the total of surcharges was 1.3308 trillion won (Fair Trade White Paper 2019, KFTC, p.109).
administrative agencies. Businesses can challenge these administrative sanctions and file a suit with the court. Generally, a criminal fine is smaller in amount compared to an administrative surcharge.

iii  Compliance programmes

As referred to above in the standard statutory language for corporate criminal liability (Section III.i), the law provides a safe harbour if the business in question fully performed its duty to supervise its corporate representative and adopted reasonable and thorough measures to prevent criminal violations by its corporate representative. Full discharge of a corporation’s duty can mitigate the criminal penalties or exempt corporations therefrom.

Although courts have yet to establish clear standards on the specific measures and actions that should be taken by corporations to be exempt from criminal punishment, the Supreme Court held, in an unauthorised building construction case, that the question of whether a corporation fulfilled its obligation to supervise its corporate representative is assessed by taking into account all the circumstances, including:

a  the intent and purpose of the law;
b  the details of the violation and the degree of damages or consequences caused thereby;
c  the size of the corporation and the feasibility of supervising individuals who commit violations; and

d  the measures or actions taken by the corporation to ensure the prevention of such violations.27

It was also held that exercising general supervision by training employees to ensure compliance with the Public Health Control Act and collecting signed pledges of compliance from employees when they joined the company does not automatically qualify a corporation for exemption from liability.28 In this regard, a corporation should:

a  periodically update its internal compliance manuals;
b  provide regular training sessions for employees;
c  evaluate factors that cause violations and analyse the business activities of each department to understand risks and conduct and tailor proportionate supervision accordingly;
d  establish an internal control and compliance system;29 and

e  conduct a thorough internal investigation and establish a policy of zero tolerance when any violation is detected.

27  Supreme Court of Korea, judgment 2009DO5516, 14 July 2011.
28  Supreme Court of Korea, judgment 92DO1395, 18 August 1992.
29  It is likely that the Supreme Court will take into account the size of the corporation and the nature of the affairs when assessing whether the corporation exercised adequate supervision over potential violation. Therefore, while smaller corporations might qualify for safe harbour through relatively simple measures, such as communicating their compliance policies and manuals, holding regular meetings and having a reporting system in place, larger corporations will have to introduce more sophisticated systems, such as information management programmes for compliance purposes or a comprehensive system linked to an existing accounting, reporting or training system.
With regard to administrative sanctions, the relevant statutes usually do not provide safe harbour for businesses. However, court precedent indicates that justifiable cause for the violation may be accepted as a defence.\(^{30}\)

### iv Prosecution of individuals

Because corporate criminal liability is not recognised under the Criminal Act and the amount of criminal fines imposed on corporations is usually not substantial, the investigating authorities generally seek to hold individuals liable first; then, if the relevant body of law contains a corporate criminal liability provision, the investigating authorities may hold the corporation liable with the evidence gathered during the investigation against the individuals. When the government investigates individuals, a corporation may coordinate with an individual’s counsel as long as such coordination does not amount to improper interference with the government’s investigation. Immediate dismissal or disciplining of the responsible employees may prove the company’s full commitment to implementing its compliance policy but, in practice, it takes substantial time before a corporation can complete the proper procedures and obtain enough evidence to undertake the disciplinary action required under South Korean labour laws. Therefore, a lack of immediate disciplinary measures against the individuals involved is usually not regarded as lack of commitment or enforcement of a compliance policy within the corporation.

When the individual representative or employee of a corporation becomes a suspect or a defendant in a criminal or civil case, the corporation cannot pay or advance the legal fees. However, if the corporation has a substantial interest in the outcome of the case, the individual’s actions were lawful, or the action was required by the individual’s position and, therefore, the corporation needs to support the case for its own interest and the amount of legal fees are reasonable, the payment of legal fees by the corporation is allowed.\(^{31}\) The court will take into account all the circumstances in determining whether the payment of such fees is proper. Although some insurance companies provide directors’ and officers’ liability compensation policies, they do not usually cover intentional violations of law or regulations.\(^{32}\)

---

30 In a case where a business allowed a minor in its video-watching room (which are adult-only facilities in South Korea), the court accepted its justifiable cause defence that because the relevant law was so complicated and self-contradictory, the business had reason to believe that the minor was legally allowed to enter the facility as a customer (Supreme Court of Korea, judgment 2001DU3952, 24 May 2002). In another case, in which an owner of a building fraudulently used the public water supply, the court accepted the justifiable cause defence because the water supply pipe in question was installed by the previous owner of the building and the current owner had no idea of the problem (Supreme Court of Korea, judgment 98DU5972, 26 May 2000).

31 Supreme Court of Korea, judgment 2007DO9679, 26 June 2008; Supreme Court of Korea, judgment 2005DO9861, 8 September 2006.

IV INTERNATIONAL

i Extraterritorial jurisdiction

Generally, South Korean authorities have no jurisdiction over conduct that occurs outside the South Korean territory and is committed by a foreign national or a foreign company unless South Korea or South Korean citizens are affected by such conduct. Likewise, the authorities do not spend significant resources concerning the conduct of companies outside South Korea, whether foreign or domestic, unless the conduct has a substantial effect on South Korea or its citizens.

ii International cooperation

The South Korean government cooperates with other countries’ law enforcement or prosecutorial functions. Although practical difficulties exist because of the language barrier and the workload created by translation within the authorities, international cooperation is becoming more common. Traditionally, these cooperative efforts have been treaty-based. However, more authorities are focusing on direct inter-authority cooperation (e.g., cooperation between prosecutorial functions, police departments, tax authorities and financial intelligence units in each country). As of December 2017, South Korea has extradition treaties with 78 countries and mutual legal assistance treaties (MLATs) with 74 countries. In practice though, extradition is permitted in only a small number of major cases. Between 2008 and 2017, South Korea requested the extradition of 27 persons and received extradition requests for seven persons on average each year. For the same period, South Korea requested MLATs for 141 cases and received MLATs for 95 cases annually. The average number of suspects repatriated into South Korea between 2014 and 2018 was 253 annually.

iii Local law considerations

Because South Korea has strict data privacy laws, companies usually have to receive a very detailed consent letter before gathering information from an employee’s digital devices. Although informal dialogue or negotiations with the investigating authority is usually permitted, formal plea bargaining or settlement with authorities is not recognised under the law, which makes it difficult for a corporation to resolve a case at an early stage. Although a suspect or defendant in a criminal investigation can receive assistance from counsel during a government interrogation, the practice with respect to the scope of permitted attorney assistance differs between agencies or individual investigators. Unless the manner in which the investigation is conducted is deemed unfair, it is usually not permitted, without the approval of the investigator, for an attorney to interrupt a conversation between the investigator and the suspect, or for an attorney to directly answer the investigator instead of the suspect. In principle, brief note-taking by a suspect, defendant or their counsel during investigations is

36 However, in a KFTC investigation, a negotiated agreement is possible. See Articles 51-2, 51-3, 51-4 and 51-5 of the Monopoly Regulation and Fair Trade Act.
37 Article 243-2(3) of the Criminal Procedure Act. The defence counsel who participates in the interrogation may make a statement of his or her opinion after interrogation, provided that the counsel may raise an objection to any unfair interrogation manner even in the middle of the interrogation and may also make a statement, with approval by the prosecutor or the police officer.
Investigators often keep asking questions even after the defendant opts to remain silent. When authorities interview a person as a witness (i.e., a person who is not a suspect or a defendant), the witness can have his or her counsel present during the interview. When an investigation is conducted by agencies other than the Prosecutors’ Office or the police and the investigation is not aimed at imposing criminal sanctions, the assistance of counsel during government interrogation is sometimes denied.

V YEAR IN REVIEW

A very stringent and thorough anti-corruption law, the Improper Solicitation and Graft Act (ISGA), was introduced in September 2016. ISGA applies to a wide scope of targets, including not only public officials and employees of state-owned enterprises but also employees of private media companies, teachers and employees of private schools, and private individuals performing public duties (hereinafter referred to as public officials). Specifically, ISGA has two major components: prohibition of the provision of economic benefits to a public official, and prohibition of improper solicitation. When the economic benefit is in excess of 1 million won at a time or 3 million won in total in one fiscal year and it does not qualify under any safe harbour clause, provision of such benefit is criminally punished regardless of its connection with the public official’s duties and his or her motive. When the economic benefit is less than the above amounts and the benefit is given in relation to the public official’s duties, unless it qualifies under any safe harbour clause, providing this benefit is punished by a surcharge regardless of whether it is provided to receive an improper advantage.

Between late 2016 and mid-2018, the corruption investigations and trials involving former President Park Geun-hye and a couple of South Korean conglomerates were major cases. The current President Moon Jae-in administration proclaimed stricter punishment against business crimes by large companies, such as the abuse of economic power or breach of trust by controlling shareholders. However, there has not been substantial increase in terms of the number of major corporate investigations so far because the authorities have put substantial resources into politically controversial cases involving high-ranking public officials.

38 The police have internal rules that allow brief note-taking by an attorney during an interrogation. Article 8(2)(4) of the Rules on the Assistance of and Interview with Counsel (National Police Agency Order, No. 702, 19 April 2013). Likewise, Article 13-10 of the Case Handling Rules of the Prosecutor’s Office permits note taking.

39 Both the Prosecutors’ Office and the police have internal rules that, in principle, allow witnesses to have the assistance of counsel during an interview. Article 9-2(8) of the Prosecutor Offices’ Rule (Ministry of Justice Order, No. 966, 31 January 2020). Article 11 of the Rules on the Assistance of and Interview with Counsel (National Police Agency Order, No. 702, 19 April 2013).

40 Although there are certain exceptions, the typical exception is: food not exceeding 30,000 won; gifts not exceeding 50,000 won (for gifts of agricultural or fishery products, not exceeding 100,000 won); and cash gifts for congratulatory or condolence purposes not exceeding 50,000 won (for wreaths or floral arrangements provided in lieu of cash gifts for congratulatory or condolence purposes, not exceeding 100,000 won) when these benefits are not provided in return for a favour or to influence the discharge of a public official’s duty. See Article 8 of the Improper Solicitation and Graft Act.
VI CONCLUSIONS AND OUTLOOK

From a global perspective, government investigations in South Korea tend to be more focused on holding the individuals liable and, with the exception of violations of competition law, monetary sanctions imposed on corporations have not been particularly harsh. There is room for growth with respect to the protection of the investigation subject’s procedural rights during an investigation, especially by broadening the scope of permitted attorney assistance during interrogations and recognising attorney–client privilege and the doctrine of attorney work-product privilege. Although international cooperation is growing, there are still obstacles owing to scarcity of public resources and language barriers.
I INTRODUCTION

The criminal courts in Spain have sole jurisdiction to prosecute criminal corporate conduct. The investigation and prosecution of criminal offences, therefore, falls to the examining magistrates’ courts, which are responsible for conducting the preliminary investigation stage in criminal proceedings. In this role they are assisted by the state law enforcement bodies.

The examining magistrates’ courts conduct preliminary enquiries that are primarily aimed at gathering information and documentation that may serve as evidence (searches, interception of communications, etc.). In these enquiries they may adopt precautionary measures to ensure that the proceedings are conducted effectively (preventive or provisional detention, bonds or attachments).

Judges are required to investigate any indication of a crime and are not restricted as to what may be found, having broad powers for the purpose. They have a duty to ascertain the facts and circumstances that allow the conduct in question to be regarded as criminal, and then to (1) investigate the defendant (identification and gathering of personal details), (2) determine the damage caused and (3) identify the person responsible.

Any investigative measures that violate fundamental rights (for instance, the interception of personal communications and searches of and dawn raids on private premises) may only be agreed to in exceptional circumstances and are subject to authorisation by the court. In addition, it is necessary to ascertain what criminal act is being investigated, and whether the use of that measure of investigation is justified and proportional within the context of the investigation. The court must oversee the organisation and implementation of the measure.

Additionally, officials of the Public Prosecutor’s Office, within the scope of their duties, may carry out investigations that result in the referral of the case in question to the relevant court authority.

Given also that the role of the Public Prosecutor’s Office includes the actual filing of criminal actions, the public prosecutor may appear in the criminal proceedings and lead public prosecution.

Other government agencies (such as the tax authorities, the National Securities Market Commission, the employment authorities or the Bank of Spain) may bring proceedings against individuals or companies in relation to other corporate conduct, adjudge them responsible for offences provided for by law and impose penalties. These agencies are able to require the production of documents and to interview individuals, as long as there is no violation of the subject’s fundamental rights.
During any administrative proceedings conducted by the aforementioned government agencies, if it is suspected that the activity constitutes a criminal offence, proceedings will be stayed and the case immediately referred to the Public Prosecutor’s Office or to the court.

The government’s criminal policy unquestionably has an impact on the prosecutorial role. This policy is influenced not only by national needs or priorities but by the international obligations that must be fulfilled by the government; however, the effects of the policy do not extend beyond the day-to-day work of the courts and investigations.

II CONDUCT

i Self-reporting

Act 5/2010 of 22 June 2010 introduced for the first time the criminal liability of legal entities. Accordingly, under Article 31-bis of Act 5/2010, a legal entity could be held criminally liable, ‘in the cases provided for in this Code’,\(^2\) for:

a

- offences committed on its behalf or for its benefit by its legal representatives and de facto or de jure directors; and

b

- offences committed on its behalf and for its benefit by persons who, in the fulfilment of their duties and subject to the authority of the aforementioned individuals, would have performed the criminal acts as a result of a lack of due control over them.

Notwithstanding the foregoing, Act 1/2015 of 30 March amending the Penal Code, which entered into force on 1 July 2015, modified the above-mentioned Article 31-bis, making corporate entities liable as follows. In the cases provided for in this Code,\(^3\) these entities will be criminally liable for:

---

\(^2\) At that time an entity could be held to be criminally liable only in the following cases: illegal trafficking of organs (Article 156-bis); trafficking of human beings (Article 177-bis); offences relating to prostitution and the corruption of minors (Title VII, Chapter V); the discovery and disclosure of secrets (Article 197.3); fraud (Title XIII, Chapter VI, Section 1); criminal insolvency (Title XIII, Chapter VII); intellectual and industrial property offences; market and consumer-related offences and the new offence of corruption between private parties (commercial bribery) provided for in Article 286-bis (all of which are included under Title XIII, Chapter XI); money laundering (Article 302); tax and social security offences (Title XIV); offences against the rights of foreign citizens and clandestine immigration (Title XV-bis); offences relating to the development and use of land (Article 319); the cases described in Articles 325 and 326 in relation to offences against natural resources and the environment; offences relating to facilities for the storage or disposal of toxic waste (Article 328); the spillage or emission of materials or ionising radiations or the exposure of people to such materials or radiations (Article 343); the handling of materials, equipment or devices that could have devastating effects (Article 348.3); offences against public health involving the growing, manufacture or trafficking of drugs provided for in Articles 368 and 369; the forgery of credit cards, debit cards or cheques and documents in general (Article 399.1-bis); bribery (Title XIX, Chapter V); influence peddling (Title XIX, Chapter VI); offences of corruption in international trade transactions (Article 445); the possession, trafficking and storage of weapons, munitions or explosives; terrorism offences (Title XXII, Chapter V) and several forms of participation in criminal groups or organizations (Title XXII, Chapter VI).

\(^3\) Act 1/2015 of 30 March also extended the catalogue of crimes that entail liability. Thus: (1) new Article 258-ter of the Penal Code states that legal persons may also hold criminal liability for the new crimes of frustration of enforcement; (2) Article 304-bis 5 also expressly states that legal entities are criminally liable for the new crime of illegal financing of political parties; (3) Article 288 provides that legal persons may also hold criminal liability for the new offence of corruption in business introduced in new Article 286-ter; (4) for its part, Article 366 of the Penal Code is amended to expand the range of crimes against public health.
a. Offences committed for and on behalf of them and to their direct or indirect benefit, by their legal representatives or by those persons who, acting individually or as members of a body of the legal entity, are authorised to take decisions on behalf of the legal entity or have organisational or management powers therein; and

b. Offences committed in the performance of corporate duties and for and on behalf of them and to their direct or indirect benefit, by those persons who, being subject to the authority of the persons referred to in the foregoing paragraph, have been able to carry out the offences as a result of the failure by the latter to fulfil their duties of supervision, monitoring and control of the activity of the former, bearing in mind the specific circumstances of the case.

The latest reform of the Criminal Code was passed by Act 1/2019 and entered into force on 13 March 2019. It didn't change the wording of the referred Article but extended the corporate criminal liability to public misappropriation offences\(^4\) and terrorism crimes.\(^5\)

As a result of these provisions, legal entities may be held to be criminally liable and must, therefore, ensure that they have suitable corporate compliance programmes in place that provide for the possibility of investigation of any internal wrongdoing, but there is no obligation to report the conduct discovered by the company. Under Article 31-quater, the criminal liability of a legal entity may, however, be mitigated in the following circumstances:

a. Disclosure of the offence to the authorities prior to learning that proceedings have been brought;

b. Cooperation by providing evidence to the investigation that is new and decisive for shedding light on the criminal liability;

c. Reparation or mitigation of any damage caused by the offence prior to the criminal trial; or

d. Prior to the trial, taking effective measures to prevent and detect any possible offences that could be committed in the future using the resources of the legal entity.

This would be reflected by a reduction in the penalty imposed in accordance with the rules set out by Article 66 of the Criminal Code, which is proportionate to the extent of the cooperation provided but will not totally exempt the company from liability.

In conclusion, although no obligation of self-reporting is established, it could have very positive results for the legal entity and must be decided on a case-by-case basis.

From a criminal standpoint, it is advisable as well as necessary that the company cooperates with the public offices in charge of the case. Such public–private cooperation will lead to a win-win situation.

In addition, although the lack of collaboration with the authorities is permitted as part of the rights of defence of the entity under investigation, according to case law this conduct will prevent the legal person from appearing in court as a private prosecution.

---

\(^4\) Section 5 of Article 435 of the Criminal Code.

\(^5\) Article 580-bis of the Criminal Code.
ii Internal investigations

As already indicated, as a result of the entry into force of Act 5/2010 and the introduction of the criminal liability of legal entities, an increasing number of companies are implementing corporate compliance programmes that set out suitable monitoring and control measures for preventing criminal conduct on the part of their directors, legal representatives or employees.

A very important part of a corporate compliance programme, which allows a business to ascertain whether sufficient controls are in place, is without doubt the internal investigation of any irregular conduct that becomes known within the company.

In other words, corporate compliance programmes must include specific measures for the prevention and detection of possible criminal offences. It should be stressed that the reform introduced by Act 1/2015 expressly set the requirements for an effectual corporate compliance programme, including reporting channels facilitating the detection of possible risks and infringements to the body entrusted with monitoring the operation and observance of the prevention model.

Thus, internal investigations are a necessary consequence of the corporate criminal liability introduced by Act 5/2010 that could be mitigated or exempted with an appropriate compliance programme in force.

For these purposes, in recent years it is becoming increasingly common for businesses to establish direct communication or reporting channels with their employees so that the latter have a means of reporting any conduct that they deem could constitute misconduct or illegal activity, or a breach or violation of laws or regulations (internal regulations of the company or legal regulations), and that has had or could have a negative impact on the business, without being afraid that disciplinary or discriminatory measures or any other actions of retaliation will be taken as a result of having reported the conduct.

In this regard, the business must establish clear and accessible communication channels that enable information to be received correctly and promptly by the relevant persons. Different information sources may be used for warning of possible irregular conduct; for example, work carried out by the internal audit department, whistle-blowing, exit interviews, rumours and employee satisfaction surveys.

That being said, there are three ways of conducting internal investigations: (1) periodical reviews of the measures implemented for the prevention and detection of possible criminal offences within the company; (2) an internal investigation started because of irregular conduct of which the entity has become aware; and (iii) a defensive investigation once a criminal proceeding has been initiated.

Nonetheless, there are no specific provisions on how to conduct internal investigations in our legal system, so they are not particularly regulated yet. Therefore, once possible irregular conduct is known, the company will investigate it in accordance with the rules set out in its guidelines on internal investigations. Normally, the person in charge of starting the internal investigation is the compliance officer.6

Corporate investigations can be conducted by both internal and external counsels. The assistance of an outside counsel will be determined according to the nature of the facts reported, the positions the wrongdoers hold and the expertise required for conducting the investigation, among others.

---

6 The compliance officer is the body within the company that has autonomous powers of initiative and control within the legal person, which existence is one of the requirements set in Article 31-bis 2 for the exemption of criminal liability.
When there is suspicion of the committing of a crime, it is always advisable to retain an outside counsel to assure independence during the course of the investigation, to guarantee the authorities the objectivity of the results achieved, as well as to preserve professional secrecy in the exchange of documentation and information.

Only outside legal counsel communications will be totally protected by professional secrecy in Spain. There is not a legal provision regarding in-house counsels – which are bound to the company (the client) by means of an employment relationship – and, therefore, are not considered independent. In this regard, although it may be thought that in-house counsels’ communications with the entity are not protected under legal privilege, that is an issue being discussed that is not yet clear.

The professional secrecy of lawyers is enshrined in the right to personal privacy and the right to a fair defence, and releases them from the obligation to report events of which they are aware as a result of the explanations of their clients, and to testify regarding those events that the accused has disclosed in confidence to his or her lawyer as the person entrusted with his or her defence. This exemption applies to the production of documents in criminal proceedings at the request of the court, and to any other measure of investigation authorised by the court for the purposes of seizure of the requested documents.

With regard to forensic professionals and external auditors who also participate and produce reports during the internal investigation, they are not strictly protected by privilege, but by the confidentiality of the information learned. Nonetheless, if they are engaged by an outside legal counsel and as part of the right of defence of the client, it could be argued that the privilege is maintained.

However, it is quite difficult to construe that other professionals besides lawyers are entitled to claim professional secrecy to refrain from being cross-examined by the court.

Thus, the question is not yet clear in Spain and, therefore, there is still much work to be done in this regard.

As per the internal investigation process, the interviewing of the persons involved, the gathering of information, the inspection – if possible, by independent third parties – of the company’s computers and servers, and the request of documentation, including any documents in the possession of third parties, etc., is fundamental and must be recorded properly. Particularly relevant is the maintenance of the chain of custody when gathering information from electronic devices during the internal investigation to be able to use it as evidence if a criminal proceeding is initiated, as well as to avoid declarations of invalidity of such evidences.

As regards the interviewing of employees and the possibility of being accompanied by a lawyer, this will depend on the policy existing at the company regarding internal investigations. In any event, it is customary, especially at the beginning of the investigation, for employees to be informed in detail of the reason for the interview, but not to retain their own lawyers. The most widespread practice is guided by the provisions of employment law, consulting with both the compliance officer and the human resources responsible regarding the specific case in question to ensure that the investigation is appropriate and proportionate and respects the rights of all parties involved.

---

7 Article 18.1 of the Spanish Constitution.
8 Article 24 of the Spanish Constitution.
9 Article 263 of the Criminal Procedure Act.
10 Articles 416.2 and 707 of the Criminal Procedure Act.
The most recent Spanish law affecting internal investigations is Act 1/2019 of Business Secrets, which entered into force on 13 March 2019, transposing the Directive 2016/943 of the European Union. The aim of the said law is to guarantee the competitiveness of the legal entities regarding investigation and innovation as well as the safe transfer of knowledge. Act 1/2019 of Business Secrets defines a ‘business secret’ as any information or knowledge that: (1) is secret (only certain employees may know about); (2) has an actual or prospective value within the company; and (3) has been duly protected with measures to remain secret. To protect the information received from a client or provider, the compliance programme of the company should include appropriate measures. Moreover, the signing of a confidential agreement between the parties should always be followed with operational measures that guarantee the maintenance of the secrecy. In such regard, Article 2.3.b regulates an exemption where the secret of the information or knowledge could be lifted: the measures, procedures and remedies provided should not restrict whistle-blowing activity. Therefore, the protection of trade secrets should not extend to cases in which a disclosure of a trade secret serves the public interest, insofar as directly relevant misconduct, wrongdoing or illegal activity is revealed.

iii Whistle-blowers

From a criminal standpoint, the figure of the whistle-blower is fairly new in our system as the criminal liability of legal entities did not apply until 2010 and was not clearly regulated until the reform of 2015, when the requirements of compliance programmes and the impact their full implementation will have on the liability of companies was specified in more detail.


In said regard, the anonymity of the whistle-blower has been finally allowed under Article 24 of this law, but preserving the confidentiality of the personal data gathered as a result of the complaint (especially, the identity of the whistle-blower, when applicable). Moreover, it states that the access to the data recorded in the whistle-blowing system is exclusively limited to ‘those who, forming or not part of the organisation, are developing internal control and compliance functions, or to those specially designated eventually. However, access by other individuals, or even the disclosure of data to third parties, could be permitted in order to adopt disciplinary measures or for judicial proceedings purposes’.

In addition, Royal Decree 11/2018, of 31 August, transposing the Fourth Directive of the European Union on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing, introduced Article 26-bis of Spanish Act 10/2010, which obligates entities to have in place appropriate procedures for their employees, managers or agents, to report internal breaches through a specific, independent and anonymous channel, proportionate to the nature and size of the obliged entity.

Whistle-blower channels should provide how the reports are received and processed. The company could decide whether the whistle-blowing channel is managed internally or by an

---

11 This law was a consequence of the implementation of the European Data Protection Regulation which became enforceable in all Member States on 25 May 2018.

12 Notwithstanding, it should be highlighted that the anonymity of the whistle-blower can make it difficult not only to duly investigate the case reported, but also to protect the whistle-blower. In addition, the employees could badly use the anonymity to report in bad faith with the sole purpose of damaging the company.
external services provider. The latter requires the signing of a confidential agreement. In such regard, Circular No. 1/2016 of Spanish General Prosecutor Office provides that monitoring and control measures appear to be more effective the higher the level of externalisation is.

If a criminal proceeding is initiated because there are grounds of the commission of a crime or crimes, the whistle-blower could turn into a witness or, in case of participation in the perpetration of the offence, into an accused party. In both cases, the anonymity of its identity could no longer be maintained.13

Although there are no incentive programmes for whistle-blowers for reporting wrongdoings to the authorities, if the whistle-blower becomes an accused party to the criminal proceedings, his or her penalty might be mitigated by the court for confession of the illegal act, according to Article 21.5 of the Criminal Code.

Lastly, it should be remarked that on 23 April 2018, the European Union published the proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law ('whistle-blower'). In case the proposal turns into a final Directive, the Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with the Directive by 15 May 2021, at the latest.14

As previously said, Act 1/2019 of Business Secrets regulated an exemption to whistle-blowers in accordance with this Directive.

III ENFORCEMENT

i Corporate liability

As has been already explained, since the entry into force of Act 5/2010, Spanish law has provided for the criminal liability of a corporate entity in certain cases (see Section II.i).

Liability of a company for a crime may exist alongside that of an individual, and the company may also be held liable when no specific individual perpetrator of the offence has been found or no proceedings may be brought against the individual (for example, because of lapse of liability by death or by application of the statute of limitation). This means that any mitigating and aggravating circumstances of either the company or the individual will not be affected by the other’s situation. This being the case, the joint representation and defence of the individual and the company may not be compatible, as it is highly likely that conflicts of interest will arise. Thus, in most cases, it may not be advisable to have a joint representation and defence in the criminal proceedings.

In addition to criminal liability, it should be remembered that there are certain civil obligations that arise as a result of criminal offences, so the ex delicto civil liability of companies exists directly and jointly and severally with that of the individuals15 and vicariously.16

---

13 Although 'protected witnesses' exist in Spanish criminal proceedings, Act 19/1994, of 23 December, on the protection of witnesses and expert witnesses in criminal proceedings, is considerably old and not effective in all cases. Notwithstanding, the circumstances to be considered as a 'protected witness' are provided in the said law and, in such case, the anonymity could be maintained.

14 One of the most remarkable provisions of the proposal of the Directive is the prohibition of any form of retaliation against whistle-blowers (Article 14).

15 Article 116.3 of the Criminal Code.

16 Article 120 of the Criminal Code.
ii Penalties

Under Article 33.7 of the Criminal Code, the penalties that may be imposed on businesses are as follows:

- a quota-based or proportional fines;
- b winding up of the company;
- c suspension of the company’s activities for up to five years;
- d closure of the company’s premises and facilities for up to five years;
- e barring from those activities through which the offence was committed, aided or concealed;
- f disqualification from public subsidies and assistance; and
- g court intervention.

Article 66-bis of the Criminal Code requires that, when applying any of the aforementioned penalties (except for fines), the judge or court will consider: (1) the need for the penalty to prevent the continuation of the criminal activity or its effects; (2) the economic or social consequences, especially for employees; and (3) the position within the company of the individual who failed to exercise due control.

The Criminal Code seeks to make fines the penalty generally applicable to businesses. The process for determining the fine, in the event of a quota system, entails the court determining the applicable fine period on the basis of the circumstances indicated in the foregoing paragraph, as well as the applicable quota for each daily fine, taking into consideration the financial circumstances of the defendant. In the case of businesses, the daily quota would range from €30 to €5,000.

Article 31-ter, introduced with Act 1/2015, provides that when both parties (legal person and individual) are sentenced to a fine in the same case on the same charges, the size of the fine each must pay is scaled so that the resulting amount is not disproportionate to the severity of the charges.

Finally, the range of potential sanctions will not vary based on the authority bringing the action.

iii Compliance programmes

As stated, Act 1/2015 of 30 March amended the Penal Code entering into force in July 2015.

Said amendment expressly acknowledged that a legal person may be exempted from criminal liability if it has a corporate compliance programme for the prevention of crime. This acknowledgement put an end to all discussion on the matter since 2010, and for the first time established the requirements that must be met by what the law terms ‘an organisation and management model for the prevention of crime’.

When a crime is committed by de facto or de jure directors or legal representatives17 of a legal person, Article 31-bis 2 of the Penal Code makes the following conditions necessary in order for the enterprise to be exempted from criminal liability:

---

17 As seen above, Article 31-bis 1a resulting of Act 1/2015 (unmodified since then) refers to ‘legal representatives or those persons who, acting individually or as members of a body of the legal person, are authorised to take decisions in the name of the legal person or hold organisation and control faculties within the legal person’.
the crime prevention model must have been adopted and effectively executed prior to the commission of the crime, including monitoring and control measures fit for preventing crimes of the sort in question or for significantly reducing the risk of such crimes;

b the crime prevention model must have been supervised by an authority that has autonomous powers of initiative and control within the legal person (a compliance officer), although when the legal person is ‘small’, supervisory functions may be assigned directly to the governing body of the legal person;

c the individuals who have perpetrated the crime must have fraudulently evaded the organisation and prevention models; and

d the authority entrusted with supervising and running the prevention model must not have failed to exercise, or insufficiently exercised its supervision, monitoring and control functions.

Article 31-bis 4 establishes that, when the crime is committed by persons provided in Article 31-bis 1(b),19 the legal person is exempted from liability if, before the crime was committed, it did in fact adopt and effectively execute an organisation and management model that was adequate to prevent crimes of the sort committed or to reduce significantly the risk of the commission of such crimes.

The Article goes on to say that partial accreditation of the criminal liability exemption requirements set in preceding Articles will be regarded as an attenuating circumstance.

Article 31-bis 5 of the Penal Code sets out the requirements for an effectual corporate compliance programme (one which is fit to qualify the legal person for exemption from criminal liability in future). Qualifying organisation and management models must:

a identify the activities in which the target crimes might be committed. In other words, before an ‘organisation and management model for the prevention of crime’ can be created, an analysis must be run that includes an in-depth examination of the company’s business, its facilities, the legislation applicable to it and to its business, etc. This analysis is what the Anglo-Saxon world calls ‘risk assessment’. The goal is to correctly identify and evaluate the company’s risk in connection with the sorts of crimes that its directors, legal representatives and employees might reasonably engage in. In short, the idea is to map out the firm’s risks;

b establish the exact protocols or procedures for forming the legal person’s wishes, making its decisions and executing its decisions in connection with its wishes. Thus, the legal person is equipped with policies, clauses, protocols and, of course, a good internal investigation manual, so that it can detect potential criminal acts;

c set up financial resource management models suitable for averting the target crimes.

The governing body’s commitment to and engagement with the corporate compliance programme must be reflected in the yearly allocation of resources so that the compliance officer can effectively carry out his or her supervision, monitoring and control functions;

---

18 According to the rewording of Article 31-bis 3 of the Penal Code, ‘small’ legal persons are those that are authorised by law to submit profit and loss accounts.

19 ‘Persons acting on behalf of the entity and for its benefit who, in the fulfilment of their duties and subject to the authority of the legal representatives and de facto or de jure directors, could have committed an offence as a result of a lack of due control’ (i.e., employees or other controlled individuals).
make it compulsory to report possible risks and infringements to the authority entrusted with monitoring the operation and observance of the prevention model. Reporting channels facilitating the detection of crimes in the company must, therefore, be implemented and all company employees must have access to the reporting channels;

establish a disciplinary system that properly penalises infringement of the measures established by the model. This condition must be seen in relation to the functions of the compliance officer and the human resources department, and it must necessarily include a reaction plan or protocol for action when a crime is committed, and the system of rules penalising crime; and

run regular verifications of the model, and modifications of the model, when evidence of major violations of the model is found or when there are changes in the organisation, the control structure or the company's business that make modifications necessary. Not only must a corporate compliance programme be introduced, but follow-up reports must also be given regularly to evaluate the design of the model and the effectiveness of the controls the company has implemented.

The latest reform of the Criminal Code (by Act 1/2019) obligates the companies to review and adapt their compliance programmes to include the new offences that may be committed by the legal entities as well as to take into consideration the stiffening of the penalties in several crimes.\(^\text{20}\)

iv Prosecution of individuals

The action of the company would vary depending on whether the offences were committed before or after 24 December 2010; in other words, depending on whether the provisions on the criminal liability of legal entities are applicable. If Article 31-bis is not applicable, the coordination of all the defences is certainly possible (and in fact, recommended) because the defence of the individual is also the defence of the company. Likewise, the payment of the employees’ legal fees is possible as the actions have been carried out by the individuals in the performance of their corporate duties. If, however, Article 31-bis is applicable, the positions of the company defence may be incompatible and the specific case must be assessed to determine whether the company may coordinate with the individual’s counsel and afford their legal fees.

According to Article 13.6 of the Code of Conduct of Spanish Legal Practitioners, lawyers should ‘refrain from managing the affairs of a group of clients affected by the same situation, when a conflict of interest arises between them, as there is a risk of violation of professional secrecy or their freedom or independence may be affected’. This provision is consistent with the fundamental right of persons to be defended and assisted by a lawyer enshrined in Article 24 of the Constitution.

The judgment 154/2016 was the pioneering Supreme Court sentence confirming the criminal liability of a corporation and also ruled that conflicts of interest could be arisen between individuals and legal persons represented in court by the same attorney. For such possible conflicts of interest, there is no general answer, but some possible formulas used in other systems are offered in case conflicts of the kind arise; for example, the judicial appointment of a ‘legal/public defender’ of the company, or the assignment of the company’s defence to the compliance officer.

\(^{20}\) For instance, tax crimes and subsidy frauds have now a lower quantity restriction: the evaded amount that leads to criminal liability has been established from €10,000 to €100,000 with different penalties.
Another matter analysed in said rulings is the possibility of the trial being annulled when the right to defence of the legal entity is breached for being represented by the natural person who is also accused individually in the same criminal proceeding.

IV INTERNATIONAL

i Extraterritorial jurisdiction


Accordingly, under criminal law, the courts have jurisdiction to hear any actions for indictable and summary offences committed in Spanish territory (principle of territoriality), notwithstanding the provisions of those international treaties to which Spain is a party. The courts may, however, also hear offences regarded under criminal law as criminal offences even though they have been committed outside the national territory, provided that those persons criminally liable are Spanish persons or foreign persons who have acquired Spanish nationality (active personality principle) after the commission of the offence and the following requirements are met:

a the offence is punishable in the place of enforcement;
b the injured party or the Public Prosecutor’s Office files a complaint or criminal complaint before the Spanish courts; and
c the offender has not been acquitted, pardoned or convicted abroad, or in the latter case, has not served a sentence.

Spanish criminal law also applies on an exceptional basis to offences committed outside the national territory, when committed by either a national or a foreign person, provided that they affect the basic interests of the state (known as the absolute principle or principle of protection of interests) or they are offences that violate the dignity of persons, transnational offences or offences committed in areas not subject to the sovereignty of any state (principle of universal justice).

In this regard, the Spanish courts have the possibility of hearing and prosecuting offences of business corruption,21 even though committed by Spanish or foreign persons outside the national territory, provided that one of the following circumstances arises:

a the proceedings are brought against a Spanish person;
b the proceedings are brought against a foreign citizen that normally resides in Spain;
c the offence has been committed by an officer, director, employee or service provider of a commercial undertaking or of a society, association, foundation or organisation that has its permanent address or registered place of business in Spain; or
d the offence has been committed by a legal entity, undertaking, organisation, groups or any other kind of entity or group of persons that has its permanent address or registered place of business in Spain.

21 These offences were globally named as ‘Crimes of business corruption’ under Act 1/2015, of 30 March. The different types of offences are provided in Articles 286-bis to 286-quater of the Criminal Code; concretely, the offence of corruption in international business transactions is regulated under Article 286-ter.
ii International cooperation

Spain cooperates with other countries in law enforcement and in prosecutorial functions not only on the basis of international treaties but also following the ‘principle of reciprocity’ enshrined in Article 13 of the Constitution.

The following European legal mechanisms for international legal assistance apply in Spain, among others:

a the Convention on Mutual Assistance in Criminal Matters of 20 April 1959, as amended by the Schengen Agreement, and the European Convention on Judicial Assistance of 29 May 2000; and

b the European Arrest Warrant regulated in the EU Council Framework Decision of 13 June 2002 and in the Spanish European Arrest Warrant Act 3/2003 (the National Court has a 24-hour service to process European arrest warrants).

In addition to the foregoing international legal cooperation (coordinated through the Spanish Ministry of Justice), the International Cooperation Unit of the Spanish Public Prosecutor’s Office is responsible for the supervision and enforcement, where applicable, of the letters rogatory addressed to or issued by the Public Prosecutor’s Office.

Likewise, this unit deals with any matter relating to the European Judicial Network, the Ibero-American Network for International Legal Cooperation (IberRED), Eurojust and the International Cooperation Prosecutors Network.

As regards extradition, Spain only grants extradition in compliance with a treaty or the law, in accordance with the principle of reciprocity. In addition, the offences for which extradition is requested must be regarded as a criminal offence under the criminal laws of both states and the sentence for the offence must be at least one year’s imprisonment. The Spanish authorities do not grant extradition for political offences.

Spain is a signatory party of the European Convention on Extradition and to a large number of bilateral treaties on extradition.

Finally, the ruling issued by the Court of Justice of the European Union on 6 September 2016 regarding the Petruhhin case clarified a controversial issue referring to extradition. In that way, it stated that if the extradition is requested by a third state (non-Member State of the EU) to a Member State in relation to a European non-national citizen of the requested state, the requested Member State should inform the state of which the European citizen is national so that the latter could adopt the decision to start a criminal proceedings against its national and, for that purpose, make a European arrest warrant to the requested state.

iii Local law considerations

Provisions exist that may restrict investigations involving multiple jurisdictions. The most relevant law in this regard is the Personal Data Protection and Guarantee of Digital Rights Act (adopted by Organic Law 3/2018 to comply with European regulations).

The international personal data disclosure (i.e., transfer of data between different states or international organisations) is subject to both the provisions of the European Regulation and the above-mentioned organic law. The main point of Spanish Act 3/2018 is the requirement of the consent of the data owner to allow for its treatment, also stating the obligation to inform him or her about all the purposes for which the personal data could be used.22

22 Article 6 of the Data Protection Act.
In addition, as previously mentioned, the disclosure to third parties of the data recorded in the whistle-blowing system could only be permitted to adopt disciplinary measures or for judicial proceedings purposes.23

For its part, Article 28.g is encouraging the increase of data protection measures in several cases such as when the personal data is disclosed, habitually, to third states or international organisations of which a proper level of protection has not been declared.

Personal Data Protection is also regulated in Articles 236-bis to -decies of the Spanish Act on the Judiciary, lastly modified by Act 7/2015, of 21 July. Under said regulation, the consent of the owner of the data is not necessary for its treatment by the courts notwithstanding procedural rules regarding the validity of the evidence.24

Finally, banking secrecy is not regarded under law as an asset or property subject to protection in itself or by itself, but as something that is merely instrumental in protecting the real legal interests that merit protection, such as privacy, free competition, business secrets or the security of the state. As a result, in recent rulings, the courts have established that the lawfulness of any information protected by secrecy, either under privacy protection or the protection of a business secret, is a fundamental factor. They have also ruled that, in any event, there are greater interests that warrant the transfer of information to certain public persons (in addition to the interested parties) who are legally authorised to know that information, such as the government authorities responsible for tax fraud and – specifically – the Public Prosecutor’s Office and the courts in the investigation and prosecution of criminal offences.

V YEAR IN REVIEW

There are no new developments in sight for the coming year in relation to internal investigations as the latest reforms of the Criminal Code adopted by Act 1/2019 of 20 February25 and Act 2/2019 of 1 March26 do not provide any provision in said regard. Notwithstanding, internal investigations are gradually making inroads in Spain as legal entities are taking more seriously the full and correct implementation of their compliance programmes to avoid or mitigate future penalties.

In addition, if the European Union proposal for a Directive on whistle-blowing finally passes into Directive, the Member States shall implement its provisions, which will affect internal investigations, because the following is regulated: (1) the obligation of setting up internal and external channels and procedures for reporting and follow-up of reports; (2) the treatment of the data gathered in the internal investigation; and (3) the penalties to be imposed upon wrongdoers.

To date, there have been 26 judgments by the Supreme Court regarding the criminal liability of legal persons. The most relevant ones could be summarised as follows.

The pioneering Supreme Court sentence (STS 154/2016) has already been mentioned in the previous Section as it is highly relevant and refers to possible conflict of interests between natural individuals and corporations.

23 Article 24 of the Data Protection Act.
24 Article 236-quater of the Spanish Act on the Judiciary.
25 Regarding the transposition of European Union directives in relation to financing and terrorism.
26 In relation to road safety offences.
The following was STS 221/2016 which ruled that, as could not have been otherwise according to the main Spanish criminal principles, a legal entity could only be criminally liable for illegal acts that took place after the reform of the Criminal Code in 2010.

The next remarkable ruling of the Supreme Court was STS 583/2017 of 19 July, which lowered the penalties imposed by the lower court, definitively establishing the criteria to follow for charging legal persons with a crime. The resolution also provided guidelines on the interpretation of penalties set forth in Article 66-bis of the Penal Code, stating that judges shall apply the proportionality principle when a legal person is convicted.

In addition, STS 489/2018 of 23 October analysed the possibility of the legal entity using its employees’ emails as evidence in the criminal proceedings. Said ruling set that the key point to determine whether or not there has been a violation of the employees’ privacy is the existence of consent granted by the employee to the employer to supervise him or her. In other words, to use the employees’ emails as valid evidence in court, a prior value judgment should be made to determine if said possibility was known and contractually permitted by the employee and, therefore, constitutes a proportional measure to investigate an offence. Otherwise, the access will only be permitted under judicial authorisation.

For its part, STS 742/2018 of 7 February 2019 is one of the most noteworthy rulings, as the Supreme Court finally answered criminal or procedural questions regarding corporate liability. As such, it stated that the death of the natural person does not prevent the conviction of the entity. Finally, the Supreme Court clarified that single-member companies could also be held criminally liable.

The following ruling (STS 746/2018 of 13 February 2019) was also notable. The Supreme Court dismissed one of the grounds of an appeal considering that the fact that the summons didn’t specify whether or not the offender should appear in court as a natural person or as representative of the entity did not prevent him form making the tax adjustment provided in Article 305.4 of the Criminal Code. Moreover, Article 31-ter 1 was applied in relation to the adjustment of the penalty between the natural and the legal person. In addition, the Supreme Court clarified that the mitigating circumstance of undue delays could not apply to the entity, but only the redress of damages specifically provided in Article 31-quater c.

Moreover, STS 123/2019 of 8 March is also relevant, because it is the ruling where the Supreme Court expressly recognised that the lack of a statement from the person designated by the company (because he was not summoned to appear in court) infringes the rights inherent to the defendant parties and therefore leads to the invalidity of the proceedings having to start over the investigation phase.

For compliance purposes, STS 192/2019 of 9 April is enlightening, where the Supreme Court makes an analysis of the compliance programmes, emphasising that they should be implemented and focused on preventing corporate crimes, not on avoiding the punishment.

The ruling 234/2019 of the Supreme Court of 8 May 2019 reiterated that the right to the presumption of innocence is also granted to legal entities as well as the rest of procedural rights recognised to individuals.

STS 499/2019 of 23 October emphasised that the defendant is not entitled to request the investigation of its own company or any other third party (given his or her condition as defendant), neither to try to avoid his or her responsibility, arguing that the company was not investigated in the proceedings.

In addition to the rulings of the High Court, which guide the lower courts, there is other remarkable case law regarding corporate criminal liability that should be highlighted.
For instance, ruling 516/2017 of the ‘Audiencia Provincial’ of Santa Cruz de Tenerife of 20 December, which acquitted a company because its right to be heard before the court was not granted, and neither was the indictment properly formulated.

VI  CONCLUSIONS AND OUTLOOK

As has already been discussed, the criminal liability of legal entities was introduced in 2010. Nonetheless, there is still little relevant case law in this field.

Since the 2015 reform, as the provisions are clearer in terms of the implementation of compliance programmes, the role of compliance officers and of internal investigations, it is anticipated that we will have more rulings from superior courts in such matters.

The latest reform, which took place in 2019, has no remarkable aspects regarding corporate criminal liability beyond the aforementioned.

Although past rulings are enlightening for the interpretation of the law, we still have a long way to go and a lot of questions to answer, such as:

- the regime for whistle-blowers, which have been partially regulated by Data Protection Law but continues casting doubts in different matters and jurisdictions;
- attorney–client privileges and work-product privilege that may apply during internal investigations;
- the impact of the collaboration with authorities beyond the possibility of applying the general mitigating circumstance in case of confession (following other jurisdictions such as the United States);
- the personal liability of compliance officers for not fulfilling their duties;
- conflicts of interest between legal and natural persons (despite the two rulings of the Supreme Court that superficially analysed such conflicts); and
- the application, in practice, of mitigating and exonerating circumstances and the like, because the case-law until now was not clear enough in this regard.27

---

27 STS 746/2018 of 13 February 2019 denied the application of the mitigating circumstance for undue delays according to the specific wording of Article 31-quater which starts with ‘only’ when referring to the mitigating circumstances that could be applied to legal persons.
Chapter 23

SWEDEN

Ulf Djurberg and Ronja Kleiser

I INTRODUCTION

The Swedish Prosecution Authority is responsible for investigating and prosecuting alleged crimes committed by individuals in companies. In particular, the National Anti-Corruption Unit (the Unit) is responsible for investigating corporate conduct in respect of bribery and closely related offences. The Unit consists of a number of specialist prosecutors and three economic accountants. The Unit closely monitors any media reports on suspected bribery and tends to investigate events that are subject to such reports. Further, the Swedish Economic Crime Authority leads and coordinates the fight against organised crime, especially in respect of tax crimes, market abuse and accounting crimes. It consists of specially trained economic prosecutors, economic police officers, economic auditors and economic administrators.

The legislative framework governing the authorities’ ability to investigate and prosecute corporate conduct consists primarily of the Swedish Penal Code and the Swedish Code of Judicial Procedure. In short, the Penal Code provides the substantive rules on criminal conduct and their consequences. The Code of Judicial Procedure provides, inter alia, the investigative measures available to the prosecutor during a preliminary investigation, such as seizure and search of premises.

In recent years, there has been a focus on giving Swedish companies stronger incentives to focus on compliance, including anti-bribery. For instance, an act ensuring the protection of whistle-blowers was adopted in January 2017. In January 2020, the maximum corporate fine was also raised from 10 million kronor to 500 million kronor (more information about corporate fines in Sweden can be found in Section III.ii). Furthermore, the focus in the European Union to provide tools to fight organised crime has resulted in the implementation of a fifth anti-money laundering directive, which applies to a larger number of operators (including cryptocurrency wallet services and cryptocurrency exchanges) than the previous directives and which offers protection to whistle-blowers who report money laundering. The fifth anti-money laundering directive has been fully implemented in Sweden since January 2020.

In other fields of law, the various Swedish authorities are empowered with different investigatory tools, such as dawn raids, frequently used by the Swedish Competition Authority and the Swedish Economic Crime Authority to investigate infringements of the Swedish Competition Act and economic crimes such as insider trading. One example of a high-profile case in this field during the past year is a case where the Swedish Competition Authority conducted dawn raids at the premises of a makeup and beauty products retailer because

---

1 Ulf Djurberg is a partner and Ronja Kleiser is an associate at Setterwalls Advokathyra AB.
of suspicions that the company had applied an exclusionary strategy to prevent potential competitors from establishing themselves in Sweden. The company has denied the allegations and the Swedish Competition Authority’s investigation is, as of May 2020, still ongoing.

II CONDUCT

i Self-reporting

There is no general obligation under Swedish law to notify or self-report wrongdoings to the authorities; however, there are a few exceptions. Since 1999, chartered accountants have been obliged to report findings to the Swedish Prosecution Authority if they suspect that a crime has been committed by a company’s management or board. External counsel is, according to EU legislation, obliged to report suspicions of money laundering or terrorist financing.

The Competition Act contains provisions on leniency and immunity from fines that may be offered to a company found to have infringed the Act if it is the first to notify the Swedish Competition Authority (the Authority) of an anticompetitive cooperation and the notification submitted by the company contains information that enables the Authority to carry out a targeted inspection. The discretion of the Authority to decide the extent of immunity and leniency is very broad. Further, when determining the reduction of fines, the Authority considers whether the evidence provided by the company represents significant added value to the investigation. Swedish legislation is based on the leniency programme applied by the European Commission.

ii Internal investigations

A company may conduct its own internal investigation at any time provided that it is made in accordance with relevant applicable legislation, such as labour protection and data protection legislation. Such investigations are often conducted within the scope of internal compliance programmes, but also if there are reasons to suspect that crimes have been committed in connection with the company’s business activities. They are often conducted by external counsel, such as legal and information technology experts, and aim to discover malpractices by reviewing data and physical documents and interviewing relevant persons in the company. There are no general rules that oblige a company to disclose findings from an investigation to the authorities.

The Swedish Corporate Governance Code (the Code) is a self-regulatory set of rules that apply to all Swedish companies whose shares are listed on a regulated market in Sweden; at present, there are two – Nasdaq Stockholm and NGM Equity. According to the Code, the board of directors is obliged to ensure that there is an effective system for follow-up and control of company operations and that there is a satisfactory process for monitoring companies’ compliance with laws and other regulations relevant to company operations as well as companies’ compliance with internal guidelines.

iii Whistle-blowers

A new act aiming to ensure the protection of whistle-blowers was adopted in January 2017 – the Act on special protection for workers against reprisals for whistleblowing concerning serious irregularities (2016:749). According to this Act, employees who report a crime that may be sanctioned with imprisonment (including the crime of giving or receiving bribes),
or thereby comparative misconduct in the course of company activities, may be awarded damages if the company imposes any kind of reprisal against the employee for reporting the misconduct. The Act applies to both monetary and social reprisals.

However, the Act does not grant a right for employees to report misconduct. Inter alia, an employee who reports serious misconduct may still be liable for damages pursuant to disclosure of trade secrets or breach of loyalty in employment agreements.

According to the Code, companies must have an internal audit function. If a company does not have a separate internal audit function, its board of directors must evaluate the need for such a function annually and justify its decision in its report on internal controls in the company’s corporate governance report.

If a company introduces special reporting channels to enable employees to report suspected non-compliance with laws or internal codes of conduct, or similar activities, this must be done in accordance with the Swedish Personal Data Act, and since 25 May 2018, in accordance with the EU General Data Protection Regulation and the Swedish Data Protection Act. According to the Swedish Personal Data Act, and unless there are justifiable reasons, only public authorities may process personal data regarding crimes, judgments in criminal cases and coercive measures in criminal proceedings. Companies are generally obliged to obtain an authorisation from the Swedish Data Protection Board to be allowed to process such data, but there is an exemption from that requirement regarding whistle-blowing systems. However, companies must still comply with the basic requirements on whistle-blowing systems with respect to the processing of personal data. This requires, inter alia, that the data processing must only concern persons in key positions of the company or the company group, the information must be proportionate with regard to the purpose of the data processing and the suspicions must concern serious offences such as auditing crimes, corruption crimes, crimes in the financial sector, serious environmental crimes, serious safety deficiencies and very serious forms of discrimination or harassment. According to the Swedish Data Protection Board, the implementation of the EU General Data Protection Regulation does not require any changes in this regard.

III ENFORCEMENT

i Corporate liability

Under Swedish law, only natural persons may be liable for criminal acts committed in the course of the activities of a company. The company itself cannot commit criminal acts. Of course, criminal acts may be committed in the course of the business activities of a company, and to this end, corporate fines may be imposed for criminal activities within a company (see Section III.ii). However, according to the Swedish Companies Act and principles derived from case law, criminal liability may be claimed from those in leading positions of a company. In principle this means that the board of directors and the chief executive officer, who are responsible for the management of the company, are liable for the company’s conduct. There are examples in Swedish case law where all board members have been found guilty of criminal acts committed within a company.

In addition to criminal liability, both natural and legal persons may be held liable to pay fines for breaches of Swedish civil law. Specific corporate regulations in this respect may be found in many fields of law (e.g., competition, consumer protection, environment and employment). In addition, responsibility may be claimed through the application of general Swedish tort law. A Swedish tort claim requires intent or negligence to be granted. Needless
to say, responsibility may also be claimed on the basis of contractual obligations. Under Swedish tort law, a company is liable for the damage caused by it, unless a representative of the company acted beyond his or her competence.

As aforementioned, a company representative may also be held criminally liable for conduct within the company’s scope of business. Such liability may in some cases be relevant for breaches of environmental and labour law. Furthermore, a representative may be held criminally liable for negligence, such as causing danger to employees or others.

In most cases, companies are also subject to civil liability caused by the actions of its employees. This includes civil liability caused by criminal acts of an employee, unless the employee acted for another company or for himself or herself as a private person. The liability is only relocated to the company if there are extraordinary reasons.

ii Penalties
As stated above, companies cannot be subject to criminal liability under Swedish law. Therefore, a prosecution directed towards alleged criminal conduct in the activities of a company must be brought against a responsible individual. However, in addition to individual criminal liability, a company may be ordered to pay a corporate fine of between 5,000 and 500 million kronor for crimes committed in the exercise of its business operations, if the corporation has not taken sufficient measures to prevent the crime, or the crime has been committed by persons supervising or controlling the business. The size of the corporate fine depends on the severity of the crime, the company’s turnover and the number of employees, so the maximum fine of 500 million kronor will only be imposed on larger companies.

Corporate fines are not regarded as a criminal sanction. The imposition of a corporate fine requires that all the prerequisites in a criminal provision have been satisfied and that someone had criminal intent in respect of the prerequisites of that provision. Corporate fines have mainly been ordered in connection with environmental and occupational safety crimes. In relation to bribery, corporate fines have not been imposed very frequently by Swedish courts and the amounts of the fines have typically been low. In 2019, there were no cases where a corporate fine was imposed in relation to bribery.

For other infringements of Swedish law (e.g., in the fields of competition, consumer protection, environment and employment), the following sanctions may be applied, depending on the case at hand: an administrative fine, forfeiture, involuntary liquidation or limitation of business operations (the latter being applicable to companies active in the welfare sector).

In contrast to these corporate sanctions, the consequences of violations of competition rules may be far worse. Infringements of the Competition Act have led to administrative fines of tens of millions of euros and the European Commission has fined companies several hundred million euros for multi-jurisdictional infringements of the relevant provisions in the Treaty on the Functioning of the European Union.

In addition, a prohibition against carrying on a business may be imposed on a person who exercises control over an undertaking that participates in certain economic crimes, meaning that person will not be allowed to hold a leading position in a company in future.

iii Compliance programmes
Compliance programmes must be regarded primarily as preventing future misconduct and may go well beyond the legal requirements. However, it cannot be ruled out that well-implemented compliance programmes may, in some cases, mitigate the assessment
of corporate sanctions, such as the amount of a corporate fine. As a corporate fine may be imposed if the corporation has not taken sufficient measures to prevent the crime, a well-implemented compliance programme could also be a way for a company to protect itself from corporate fines (however, if the crime was committed by a person supervising or controlling the business, a fine may still be imposed even if there were efficient compliance routines in place).

In contrast, poorly implemented compliance programmes or the absence of one may have an adverse effect in some cases. For example, when conducting business in high-risk areas, large enterprises are expected to have extensive compliance programmes and codes of conduct to prevent, inter alia, corruption crimes. A lack of such programmes may have an adverse effect in legal proceedings and shift some of the responsibility to managers, the board of directors or the enterprise itself. The effects of compliance programmes must therefore be assessed on a case-by-case basis.

Compliance programmes or similar instruments for the company’s compliance with laws and regulations are mandatory for some companies. As aforementioned, the Code, which applies to all Swedish companies whose shares are listed on a regulated market in Sweden, stipulates that the board of directors must ensure that there is a satisfactory process for monitoring the company’s compliance with laws and other regulations relevant to company operations.

iv Prosecution of individuals
Not all breaches of the Penal Code result in dismissal of the employee. In fact, according to the legislature, the starting point is that crimes by employees outside their employment do not constitute a breach of the employment contract. However, crimes that may seriously harm the employer may be sufficient to motivate a dismissal.

The burden of proof in relation to dismissals and terminations of employment contracts on account of suspicions of criminal behaviour is set very high. In one case, the Swedish Labour Court held that the burden of proof for dismissal of an employee suspected of bribery is as high as it would be in a criminal proceeding.

In other cases, the employer and the employee who is suspected of a crime may have corresponding interests, for example if a high-level member of management is suspected of crimes in the performance and in the best interests of the company’s business activities. Such cases often involve investigatory measures within the company’s business premises and a risk of serious harm to the company’s reputation. The company may then hire external counsels to undertake an internal investigation or to defend its employees in the court proceedings. Normally, however, a public defender is appointed to defendants and paid for by the state.

If the company pays for legal fees or damages for its employees, that payment shall be regarded as a taxable benefit.

IV INTERNATIONAL
i Extraterritorial jurisdiction
The main principle is that Swedish courts have jurisdiction in relation to crimes committed in Sweden or having its effects there. The courts also have jurisdiction in relation to crimes committed by Swedish citizens or individuals domiciled in Sweden, irrespective of where the
crime was committed. Swedish jurisdiction also exists where the crime was directed towards a Swedish legal or natural person. Unlike many other states, Sweden has not been unwilling to prosecute crimes committed outside its territory.

Under the Penal Code, there are eight specific provisions giving courts jurisdiction for crimes committed outside Sweden. For example, one of these provisions ensures that Sweden has jurisdiction over crimes that can be regarded as committed against the Swedish state, such as tax and corruption crimes.

There are no particular rules regarding the geographical scope of corporate or directors’ liability. However, if Swedish legislation affecting a company has extraterritorial application, the directors would need to ensure the company’s compliance with that legislation to avoid the risk of enforcement of it by the Swedish prosecutor.

ii International cooperation

There is close cooperation between the Nordic countries (Iceland, Norway, Denmark, Finland and Sweden) regarding recognition and completion of judgments and penalties. The close similarity of the respective criminal laws of these states has enabled such cooperation, meaning, inter alia, that coercive actions ruled from a court of one of these states can be executed in another.

There are also a number of aspects related to membership of the European Union. One aspect is the effects of the Schengen Agreement, which applies to most EU Member States, Norway, Iceland, Liechtenstein and Switzerland. The Schengen rules provide for less internal border control within the European Union and harmonised rules for crossing external borders. Also, EU Member States have extensive police and judicial cooperation through Europol and Eurojust. Further, there is an EU convention that simplifies the extradition procedure between Member States. EU cooperation also governs the right to legal counselling, compensation to victims of crime, exchange of information in criminal registers, the protection of personal data, legal assistance in criminal matters and a strategy for criminality on the internet.

In addition, Sweden has numerous bilateral extradition treaties and multilateral conventions governing the mutual recognition of foreign rulings, etc.

iii Local law considerations

In general, the relevant Swedish authorities will provide assistance in criminal matters to another requesting state even if Sweden does not have an agreement on legal assistance with that state (i.e., there is no requirement for reciprocity). However, assistance is strictly limited and requires double criminality for the execution of some coercive measures (i.e., it is required that the act for which the request relates corresponds to a crime under Swedish law). However, exceptions are made from this requirement in cases of serious offences regarding requests from an EU Member State or from Iceland or Norway.

V YEAR IN REVIEW

i Changes in Swedish legislation

As pointed out above, there has been a focus on giving Swedish companies stronger incentives to focus on compliance, including anti-bribery issues, in the last couple of years. New rules on whistle-blower protection have been implemented and the maximum corporate fine has, rather dramatically, been raised from 10 million to 500 million kronor as per January 2020.
The Scandinavian Anti-Corruption Institute, a non-profit organisation founded in 1923, publishes a Business Code that complements and clarifies the Swedish Penal Code with regard to bribery and bribery related crimes relating to companies' business activities. The Business Code is developed together with the Institute's principals (including the Stockholm Chamber of Commerce, the Swedish Association of Local Authorities and Regions and the Confederation of Swedish Enterprise). The Business Code is currently undergoing revision and a new, amended version is planned to be published in 2020. A draft of the new Business Code has been circulated among several stakeholders and the proposed new version places a stronger focus on preventive measures, including risk assessment and third-party due diligence. The code is widely accepted to constitute best practices in the anti-corruption field, especially for large Swedish corporations.

In March 2020, the Swedish Supreme Court passed its judgment in a case that has attracted much attention within the Swedish cultural sector. Two organisations in the cultural sector arranged annual gala dinners where high-ranking officials from Swedish cultural authorities were invited. During the events, guests were treated to a free three-course dinner with alcohol and entertainment included. Representatives of the organisations were prosecuted for giving bribes and the recipients were prosecuted for taking bribes. The defendants were acquitted by the District Court that first tried the case but convicted for bribery by the Court of Appeal. Hence, the expectancy was on the Supreme Court judgment to clarify under which circumstances it may be considered to constitute bribery when a public official is invited to events hosted by actors in the private sector. The Supreme Court found that the term ‘improper benefit’, which is used in the Swedish Penal Code to describe the type of benefits that may constitute bribes, is vague and that caution should therefore be applied when interpreting the term for legality reasons. According to the Supreme Court, only benefits that clearly go beyond what is acceptable should be considered as improper. When assessing whether a benefit is improper it is also important to consider whether or not the benefit was given in an open and transparent manner. The Supreme Court assessed that the dinner invitations had not constituted improper benefits and acquitted the defendants.

After five years of investigation, three former members of the senior management of TeliaSonera, including the former chief executive officer (CEO), were prosecuted in September 2017 for gross bribery in relation to the 2012 TeliaSonera affair. The allegations involved corruption crimes in connection with telecommunications company TeliaSonera's establishment of business in Uzbekistan. TeliaSonera had previously entered into settlements with Dutch and US authorities concerning the affair and paid approximately 7.7 billion kronor in fines. The affair forced several members of the management team (including the CEO) and the board of directors to resign. Further, the former CEO was denied discharge from liability at the annual general meeting in April 2014, which is very unusual to a Swedish 'large cap' listed company. However, in February 2019, the District Court acquitted the defendants, as the prosecutors had not proven that the person who handled the transactions with TeliaSonera, and who had connections to former Uzbek President Islam Karimov, held any official position or was in a position of trust within the Uzbek telecommunications sector. As the events took place before 2012, the case was tried against the earlier wording of the Swedish Penal Code, according to which the definition of bribery was narrower than under the current legislation. This meant that fewer people were encompassed by the legislation at
the time. The prosecutors have appealed the judgment to the Court of Appeal which was due to try the case in January 2020. However, the trial was postponed and following the covid-19 outbreak it is uncertain when it will take place.

The Swedish telecom company Telefonaktiebolaget LM Ericsson (Ericsson) has been investigated by US authorities for conspiring to violate the Foreign Corrupt Practices Act by bribing government officials, falsifying books and records, and failing to implement reasonable internal accounting controls in the countries Djibouti, China, Vietnam, Indonesia and Kuwait. At the end of 2019, it was announced that a settlement, under which Ericsson undertook to pay more than US$1 billion in fines, had been reached. Shortly thereafter, a prosecutor at the Unit confirmed to Swedish press that a preliminary investigation (an investigation aiming to discover if there is sufficient evidence of a crime to prosecute any individual) had been initiated by the Unit. As of April 2020, the investigation has not yet resulted in any prosecution, but the investigation is still ongoing.

VI CONCLUSIONS AND OUTLOOK

Starting this year, the maximal corporate fine has been raised substantially. Historically, we have not seen a great number of cases where corporate fines have been imposed in relation to bribery, but it is possible that the new rule will result in a higher number of cases in the future. Of particular interest will also be the outcome in the above-described TeliaSonera and Ericsson cases. As the Unit only has a limited number of prosecutors and as these cases will be time-consuming, a large share of the Unit’s resources will be focused on those cases during 2020 and the outcome will in all likelihood attract substantial media attention.

Looking forward, the implementation of the EU Directive (2019/1937) on the protection of persons who report breaches of Union law in 2021 will most likely strengthen the rights of whistle-blowers in Sweden. The legislative changes that will need to be conducted to implement the directive may furthermore lead to increased reports of misconduct within Swedish organisations and companies. Also, many companies and organisations lacking whistle-blower systems today will most likely have to implement such systems when the directive has been implemented.

Finally, we have during the past few years seen a strong trend of Swedish companies focusing more on compliance and corporate social responsibility (CSR) issues. Investors, in particular, have been more interested in these issues and due diligence processes in M&A transactions now regularly cover anti-corruption and compliance questions. This development is very positive and we both hope and believe that companies’ interest in preventing and investigation compliance and CSR issues will continue to grow.
Chapter 24

SWITZERLAND

Bernhard Lötscher and Aline Wey Speirs

I INTRODUCTION

Owing to Switzerland’s political structure as a confederation of – in many respects – sovereign states (cantons), the competence to investigate and prosecute criminal conduct in general, including unlawful corporate conduct, may lie with cantonal or with federal authorities, depending on the specific circumstances of the case.

The Criminal Procedure Code (CPC) stipulates that the cantonal criminal justice authorities shall prosecute and judge offences under federal law, unless a statutory exception applies. The exceptions to this rule, however, are many. The federal authorities typically have jurisdiction in matters concerning the interests of the confederation, such as:

1. Offences committed against persons protected by international law;
2. Offences committed against federal magistrates;
3. Acts infringing Switzerland’s sovereignty, neutrality or economic interests;
4. Offences that pose a severe threat to the public; or
5. Offences that threaten the proper functioning of the federal political system.

Of greater practical significance, however, is reserving jurisdiction to the federal authorities in economic crime matters when a substantial part of the unlawful conduct has occurred abroad or in two or several cantons with no clear local focus of the criminal activity. Such matters may include the forming of a criminal organisation, money laundering, terrorist financing and corruption, and general offences against property interests. The federal judiciary is also competent to investigate and prosecute insider trading and manipulation of the market price of securities admitted to trading in Switzerland.

The authority generally competent at the federal level to investigate and prosecute criminal conduct is the Office of the Attorney General (OAG). Matters in the field of

---

1 Bernhard Lötscher is a partner at CMS von Erlach Poncet Ltd and Aline Wey Speirs is a partner at Altenburger Ltd legal + tax.
2 Swiss Criminal Procedure Code (CPC, SR 312.1).
3 See: Article 22 CPC. The provision roots in Article 123, Paragraph 2 of the Swiss Constitution, which directs that the cantons are responsible for the organisation of the courts, the administration of justice in criminal cases as well as for the execution of penalties and measures, unless the law provides otherwise.
4 E.g., members of the federal government, the federal parliament or the Federal Supreme Court.
5 E.g., offences involving the use of explosives, toxic gas or radioactive substances.
6 Article 23 CPC.
7 Article 24 CPC.
8 Articles 154 to 156 of the Financial Market Infrastructure Act (SR 958.1).
economic crime are being handled by a dedicated division. Likewise, cantons with major financial centres, such as Basle, Ticino, Geneva and Zurich, have special units in charge of investigating and prosecuting economic crime.

The powers of investigation by prosecutors at both federal and cantonal levels are defined by federal law, namely the CPC. They comprise the range of compulsory measures typically available to public prosecutors to secure evidence, ensure that persons attend the proceedings and guarantee execution of the final judgment, in particular summons, tracing of persons and property, remand and preventive detention, searches of records, persons and premises (including dawn raids), seizure and confiscation, DNA analysis and covert surveillance (including surveillance of post and telecommunications, monitoring bank transactions and undercover investigations).

Offences in the financial sector may also trigger regulatory action by the Financial Market Supervisory Authority (FINMA) for contravention of financial markets laws, such as the Anti-Money Laundering Act (AMLA), the Financial Market Infrastructure Act and the Banking Act.

Investigations of suspected violations of regulatory laws are often assigned to independent examiners (typically a law firm or an audit firm with expertise in the field at issue); however, these examiners act under the auspices of FINMA. While neither the examiners nor FINMA agents have the power to carry out dawn raids or to search the premises of a financial institution, the law directs the parties subject to an investigation to fully cooperate with FINMA, to allow examiners access to premises and to provide them with all the information and documents that they may require to fulfil their tasks. Thus, in practice, examiners and investigating agents of FINMA have extensive investigative powers.

At the initial stage of regulatory intervention, it is not uncommon that FINMA will order an institution to conduct an internal investigation (mostly assisted by external legal and forensic experts) and to furnish a written report on the findings so as to enable FINMA to make an early assessment of the matter prior to assigning its own resources to the case.

FINMA and the competent federal or cantonal prosecution authorities may exchange information, and they are directed by the law to coordinate their investigations. Moreover, if FINMA obtains knowledge of felonies and misdemeanours pursuant to the Criminal Code (CC) or of offences against penal provisions of financial market acts, it is under a duty to report to the competent prosecution authorities.

FINMA has no powers to impose penal sanctions such as fines. However, it may respond to contraventions of regulatory rules with severe administrative measures.

---

9 Article 196 CPC.
10 The scope of regulatory jurisdiction and the powers of FINMA are specified in the Financial Market Supervision Act (FINMASA, SR 956.1).
11 Federal Act on Combating Money Laundering and Terrorist Financing (SR 955.0).
12 Federal Act on Banks and Saving Banks (SR 952.0).
13 Articles 29 and 36 FINMASA.
14 Article 38, Paragraphs 1 and 2 FINMASA.
15 Swiss Criminal Code (CC, SR 311.0)
16 Article 38, Paragraph 3 FINMASA. Violations of the criminal provisions of the financial market acts are generally prosecuted by the Federal Department of Finance or, in cases where a matter may be subject to a custodial sentence, by federal or cantonal prosecutors; cf. Article 50 FINMASA.
17 See: Articles 31 et seq. FINMASA.
Suspected unlawful restraints of competition pursuant to the Cartel Act (CartA)\(^\text{18}\) are investigated by the secretariat of the Competition Commission (COMCO). The secretariat has far-reaching investigative powers. It may, without prior court approval, order production of documents and information, carry out witness hearings, interview managers and staff of enterprises believed to be involved in a cartel or other restraints of competition, conduct dawn raids, demand expert reports and seize evidence.\(^\text{19}\)

In line with international law protecting civil rights,\(^\text{20}\) Swiss law recognises that no one must be held to incriminate himself or herself (\textit{nemo tenetur se ipsum accusare}). The CPC expressly confirms this principle, specifying that the accused party is entitled to refuse to make a statement or cooperate in criminal proceedings.\(^\text{21}\) However, this principle does not apply in administrative investigations, such as those conducted by FINMA or COMCO.\(^\text{22}\)

What is more, in the context of criminal investigations in a corporate context, the \textit{nemo tenetur} principle is subject to important limitations.

Swiss criminal law is characterised by the premise that an enterprise, subject to certain exceptions, cannot be held criminally liable.\(^\text{23}\) The investigation and prosecution of unlawful conduct is thus often directed against employees only, so that the enterprise, not being in a position to make use of the defence rights of an accused party, cannot refuse to cooperate with the prosecuting authorities. Where undertakings are subject themselves to criminal liability,\(^\text{24}\) they enjoy the same procedural guarantees as Swiss law would grant to any individual. Because the procedural rules make a distinction between the accused enterprise and those directors, officers and employees who can be called upon by the prosecuting authorities as information persons or witnesses, the options for enterprises to prevent disclosure of internal matters is nevertheless limited. Also, cooperation may be condoned by mitigating sanctions or by not sanctioning the undertaking at all.\(^\text{25}\) Last but not least, refusing to cooperate is rarely beneficial: a protracted investigation persistently absorbs management capacity, often disrupts business relationships, erodes reputation and creates legal and financial uncertainties.

\(^\text{18}\) Federal Act on Cartels and Other Restraints of Competition (SR 251).
\(^\text{19}\) See, in particular, Articles 40 and 42 of the Cartel Act (CartA).
\(^\text{20}\) See Article 14, Paragraph 3(g) of the International Covenant on Civil and Political Rights and Article 6 of the European Convention of Human Rights.
\(^\text{21}\) Article 113, Paragraph 1 CPC.
\(^\text{22}\) In conjunction with FINMA and Competition Commission (COMCO) investigations, the targeted party is subject to a comprehensive duty to cooperate (Articles 29 and 36 FINMASA and Article 40 CartA).
\(^\text{23}\) The principle known as \textit{societas non delinquere potest} was abolished in Swiss criminal law only on 1 October 2003, when Article 102 CC on corporate criminal liability entered into force.
\(^\text{24}\) Pursuant to Article 102, Paragraph 2 CC, undertakings may be held criminally liable for participation in a criminal organisation (Article 260-ter CC), financing of terrorism (Article 260-quinquies CC), money laundering (Article 305-bis CC) and bribery (Articles 322-ter, 322-quinquies, 322-septies, Paragraph 1 or 322-octies CC).
\(^\text{25}\) Articles 47 et seq. CC.
II CONDUCT

i Self-reporting

As mentioned in Section I, Swiss law recognises the *nemo tenetur* principle. This rule also applies to legal entities.26

For undertakings active in the field of financial intermediation27 and legal entities that trade in goods commercially and accept cash in so doing, Swiss anti-money laundering legislation provides for an important exception: they must report suspected money laundering, or connections to terrorist financing or criminal organisations to the Money Laundering Reporting Office of Switzerland (MROS).28 This reporting duty also exists in cases where the undertaking itself is involved in the money laundering transaction. Non-compliance may entail a fine and, more importantly, regulatory sanctions.

Within the ambit of administrative (regulatory) law, the Financial Market Supervision Act (FINMASA) requires supervised persons and entities and their auditors to immediately report to FINMA any incident that is of substantial importance to the supervision.29 The incidents referred to by the FINMASA comprise significant cases of unlawful conduct, including criminal acts such as the embezzlement of clients’ assets, disloyalty, criminal mismanagement, money laundering or large-scale tax offences.

Although Swiss cartel law does not stipulate a self-reporting duty, it strongly encourages undertakings to report unlawful restraints by providing for leniency, which ranges from a mere reduction to a full waiver of (administrative) sanction payments.30 Against the background that sanction payments under the CartA may amount to 10 per cent of the turnover achieved in Switzerland in the preceding three financial years, the incentive for undertakings to report is a strong one. Indeed, leniency applications (which necessarily require admission of own wrongdoing) are a common phenomenon in cartel law investigations. The criteria for assessing sanctions, and likewise the conditions and procedures for obtaining partial or complete immunity from sanctions, are set out in detail in an ordinance of the Swiss government, so that applicants may determine with a reasonable degree of certainty if and to what extent they may profit from self-reporting and cooperation.31

26 In spring 2018, the OAG proposed supplementing the CPC with provisions that would allow for a deferred indictment of undertakings based on deferred prosecution agreements. The prerequisites for an agreement on a deferred indictment, according to the concept, would be self-reporting or a rapid response to a criminal investigation and full cooperation with the law enforcement agencies. The undertaking would also have to recognise the facts and circumstances relevant to the criminal assessment of the conduct and any civil claims, but it would not be required to make a formal admission of guilt. The proposal is not part of the current legislative process to update the CPC, and if and when it will become law is thus entirely undecided. Once introduced, the option to obtain a deferred indictment would, however, significantly impair the practical significance of the *nemo tenetur* principle.

27 Financial intermediaries include banks, investment companies, insurance companies, securities traders, central counterparties and securities depositories, providers of payment services, casinos and asset managers.

28 Article 9 of the Anti-Money Laundering Act. The Money Laundering Reporting Office of Switzerland is a member of the Egmont Group, which is an international association of financial intelligence units, whose objective is to foster a secure, prompt and legally admissible exchange of information to combat money laundering and terrorist financing.

29 Article 29, Paragraph 2 FINMASA.

30 Article 49a, Paragraph 2 CartA.

31 See: Ordinance on Sanctions Imposed for Unlawful Restraints of Competition (Cartel Act Sanctions Ordinance, SR 251.5).
ii Internal investigations

The need to tackle suspected or actual irregularities by way of an internal investigation typically originates from diligence duties imposed by civil and administrative (regulatory) law.

As already noted, undertakings subject to supervision by FINMA are obliged to report incidents that are material from a regulatory perspective. If a matter that comes to the attention of a supervised undertaking potentially meets that criterion, the undertaking will have to clarify the pertinent facts and assess them in respect of the need to take action, including, besides reporting to FINMA, possible measures to restore compliance.

At the civil law level, an internal investigation may become imperative for board members and senior managers of an undertaking to fulfil their duty to ascertain compliance with applicable governance standards. The Swiss Code of Obligations provides that members of the board and others engaged in managing an entity’s business must perform their duties with all due diligence and safeguard the interests of the undertaking in good faith. Hence, indications of material misconduct must lead them to initiate an internal investigation.

An aspect to be given due consideration in the context of internal investigations is the protection of employees’ rights. Though it is widely recognised in Swiss doctrine and practice that communications of employees that relate to the performance of their work may be searched without their knowledge or specific consent if the prevailing interests of the employer so require, the principle of proportionality and the privacy rights of the employees must be respected. Hence, any analysis of the contents of correspondence should be preceded by a process that permits the separation of potentially relevant communications from those that are unlikely to require review. Searching communications is also relevant under data protection law. In particular, the analysis of data for communication patterns and the disclosure of personal data to third parties may be unlawful unless justified by an overriding interest of the employer.

As a result of their general obligation of loyalty to their employers, employees must cooperate in an internal investigation, inter alia, by undergoing interrogation, unless they would thus incriminate or expose themselves to civil (or criminal) liability. To enable employees to adequately exercise their rights and – not least – to create an atmosphere of mutual confidence promoting their willingness to cooperate, undertakings should, and in practice regularly do, encourage employees to retain independent counsel. Related costs are typically covered by the employer.

Confidentiality is a key requirement in not prematurely narrowing down the number of options for an adequate response to the findings that may result from an internal investigation. This applies even in cases where the undertaking may ultimately have to share its findings with the (regulatory) authorities or proceed to voluntary self-reporting. To ensure confidentiality, undertakings regularly retain law firms to lead internal investigations. Provided that the

33 See: Article 717 CO.
34 Articles 328 and 328b CO.
35 Federal Act on Data Protection (FADP, SR 235.1).
36 Articles 12 et seq. FADP.
37 Article 321a, Paragraph 1 CO.
38 Swiss law does not recognise a legal privilege of in-house counsels and legal advisers who are not members of the Bar Association, even if the work they perform may qualify as legal advice.
investigation is a task embedded in the law firm’s advisory or legal representation mandate, attorney–client privilege protects communications between the law firm and the undertaking, and between the law firm and its agents (namely, accounting and forensic firms instructed by the law firm to perform certain tasks under its auspices), and documents such as minutes of interviews conducted by the law firm, meeting notes and reports.

Recent Swiss case law underlines the importance of placing an internal investigation into the wider context of specific attorney work if confidentiality is of concern. Business undertakings cannot simply ‘outsourc’ investigations and the keeping of records of an investigation’s results to law firms to preserve privilege. Attorney–client privilege applies comprehensively only when the collation of facts, their interpretation and legal analysis are inseparable elements of one and the same comprehensive (advisory or defence) mandate.

iii Whistle-blowers

After seven years of legislative work, the plan to introduce to existing laws specific provisions on whistle-blowing in the private sector failed. In spring 2020, the Swiss parliament downed the proposed legislation. The draft bill, in essence, provided for a three-step process comprising mandatory internal reporting and the involvement of public authorities, which a whistle-blower had to observe before reporting to the public. The process was criticised as being overly cumbersome and offering insufficient protection by organisations such as Transparency International. Considering that the proposed regulation was not perfect, but still viable, the government warned in vain during the final parliamentary debate in March 2020 that no new proposal would be forthcoming for years, should the bill eventually fail.

Whistle-blowing in the private sector will, thus, continue to be governed by the general rules and principles of employment law, company law, criminal law and data protection law. An employee must raise suspected or known irregularities with his or her employer according to applicable internal rules (if any) prior to releasing any information to external entities, and thereby incur the risk of retaliation; otherwise, the employee may be in breach of contractual loyalty and confidentiality obligations towards the employer. Criminal liability may ensue in addition to the liability for breach of contract. This leaves the dilemma for whistle-blowers unsolved. Whether or not disclosure to authorities or to the public is legal continues to be decided by the courts on a case-by-case basis; an incalculable risk for potential whistle-blowers, and a situation that is at odds with Organisation for Economic Co-operation and Development (OECD) guidelines.

As, in effect, Swiss law does not require undertakings to set up a specific internal whistle-blowing unit to which employees may report confidentially, nevertheless, in line with international guidelines and best practices, many corporations have introduced a mechanism or designated an independent body to which suspected misconduct can be reported. Studies show that the number of companies having introduced a reporting point has remained unchanged during the past few years (about 11 per cent). Considerable differences exist

41 See: www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=48524#votum12.
between large international corporations where the majority of the designated internal or external reporting points are to be found (71 per cent) and smaller to medium-sized enterprises where such reporting points are still rare (less than 10 per cent). According to representative studies, the key reasons for not introducing a reporting point are the absence of a mandatory regulation and a general scepticism as to the effectiveness or advantage to the company itself.

The case law of the Federal Supreme Court provides guidance, in particular with respect to the requirements that employees must meet before reporting to the public. First, employees are bound not to disclose to the public any information concerning their employer and its business that is not in the public domain. Generally, employees must remain silent even about offences committed within the employer’s domain unless there is a public interest in the disclosure that overrides the employer’s interest in keeping unlawful conduct confidential. The proportionality test requires that an employee informs the employer before notifying the authorities and, further, that employees may report to the public only if the notified authorities fail to take action.

The public sector is ahead of the private sector regarding protection of whistle-blowers. Since 2011, employees of the federal government must report criminal conduct to the penal authorities and may inform the Swiss Federal Audit Office about suspected irregularities. In 2017, the federal government introduced an official and secured digital platform where public employees or private persons may report suspected misconduct anonymously. Since the introduction of the platform, the number of reports has increased significantly.

The Swiss Federal Police (Fedpol) is operating a web-based platform for reporting suspected corruption. The platform safeguards the anonymity of the person reporting and stores neither the IP addresses, time nor the metadata that may allow identification of the person or of the computer used to make the report. Fedpol reviews each report for criminal relevance before forwarding it to the competent internal office, external agency (e.g., cantonal police) or, in the case of irregularities within the federal administrative units, to the Federal Audit Office for follow-up action.

Non-government organisations, such as Transparency International, promote the importance of whistle-blowing in the fight against commercial crime and corruption, and advocate ensuring that whistle-blowers are afforded proper protection and disclosure opportunities under the law.

Despite the absence of whistle-blower legislation in Switzerland, Swiss companies are advised to take guidance in generally accepted practices when shaping their own whistle-blowing policies. To encourage internal reporting, companies should, in particular: (1) designate an independent whistle-blowing unit; (2) specify rules of procedure to follow up on reported irregularities; (3) prohibit dismissal or disadvantages because of reports; and (4) allow for anonymous reports.

---

43 See: DFT 127 III 310, 30 March 2011, consid. 5.
44 Article 22a Federal Act on Personnel (BPG, SR 172.220.1).
45 See: www.efk.admin.ch/de/whistleblowing-d.html.
46 See: www.whistleblowing.admin.ch.
47 From around 70 reports in previous years to 148 reports in 2019.
48 See: www.fightingcorruption.ch.
III ENFORCEMENT

i Corporate liability

Criminal law provides for a general ancillary liability of an undertaking for felonies or misdemeanours committed in its business domain if it is not possible to attribute the wrongful act to any specific individual perpetrator because of inadequate organisation by the undertaking.51 Moreover, an undertaking may be subject to criminal liability, irrespective of the liability of any individual perpetrator, for participation in a criminal organisation (Article 260-ter CC), the financing of terrorism (Article 260-quinquies CC), money laundering (Article 305-bis CC) or bribery (Article 322-ter, 322-quinquies, 322-septies, Paragraph 1 or 322-octies CC) if it is found to have failed to take all reasonable organisational measures required to prevent such an offence.52

The law on corporate criminal liability thus sanctions organisational deficiencies rather than the criminal conduct (for which the individual perpetrator remains responsible), thereby creating a strong incentive for undertakings to establish sound compliance and government standards.

Swiss law is rooted in the principle that all acts – including unlawful conduct – of board members or senior managers committed in their official capacity are deemed to be acts of the undertaking itself and may therefore expose the undertaking to civil liability.53 Likewise, an undertaking is subject to civil liability for any loss resulting from acts of employees unless it proves that it has taken all precautionary measures required in the circumstances to prevent the respective loss.54 Non-compliance with statutory duties by members of the board or senior managers (including the duty to ascertain adequate organisation of the undertaking and effective overall supervision regarding compliance with the law, the articles of association, operational regulations and directives) may also trigger the personal civil liability of board members.55

ii Penalties

Undertakings may be fined up to 5 million Swiss francs for criminal conduct that occurs in their domain.56 Moreover, assets that have been acquired through, or that are intended to be used in, the commission of a criminal offence (e.g., bribes) are subject to disgorgement.57

Contraventions of regulatory rules in the financial sector are primarily sanctioned by measures aiming to restore compliance with the law to protect either the public or the good functioning of financial markets. The array of instruments available to FINMA comprises corrective measures such as cease and desist orders, declaratory rulings, disqualification of the individuals responsible from acting in a management capacity at any undertaking subject to FINMA’s supervision for up to five years, publication of supervisory rulings, confiscation of profit made through a serious violation of supervisory provisions, revocation of licence, withdrawal of recognition or cancellation of registration and compulsory dissolution.58

51 Article 102, Paragraph 1 CC.
52 Article 102, Paragraph 2 CC.
53 Article 55, Paragraph 2 Civil Code.
54 Article 55, Paragraph 1 CO.
55 Article 754 CO.
56 Article 102 CC.
57 Articles 70 et seq. CC.
58 Articles 31 et seq. FINMASA.
addition, anyone who wilfully disregards licensing, recognition or registration requirements as set forth in financial markets legislation, wilfully provides wrong information to FINMA, auditors or self-regulating organisations, or wilfully avoids mandatory audits of financial statements by refusing to fully cooperate with auditors or FINMA’s agents, as the case may be, is liable to a custodial sentence of up to three years or a monetary penalty. Negligent conduct may be fined up to 250,000 Swiss francs. Non-compliance with FINMA rulings is subject to a fine of up to 100,000 Swiss francs.59

COMCO may sanction undertakings that have participated in a cartel or unlawful vertical restraints, or that have abused their dominant position in the market, by charging up to 10 per cent of the turnover achieved in Switzerland in the preceding three financial years. The same sanction may be imposed by COMCO on undertakings that breach an amicable settlement made with, or a final and non-appealable ruling issued by, COMCO or an appellate body.60 In the event of a breach in the context of merger control matters, COMCO may charge up to 1 million Swiss francs, or, in the case of repeated non-compliance, up to 10 per cent of the combined turnover that the undertakings concerned have achieved in Switzerland.61 Undertakings that fail to fulfil their obligation to provide information or produce documents to COMCO are subject to a charge of up to 100,000 Swiss francs.62 In addition, COMCO may fine individuals up to 100,000 Swiss francs.63

### iii Compliance programmes

The existence of an adequate compliance programme is a key defence to corporate criminal liability. As noted above, Swiss law does not hold undertakings criminally liable for offences committed by individuals within their domain, but for their failure to take all organisational measures required to prevent such offences. Among the measures required, compliance programmes have a pivotal role.64

From a regulatory perspective, compliance policies are an indispensable element of the mandatory internal control system of undertakings supervised by FINMA. Failure to establish a compliance programme constitutes a breach of the regulatory duty to ensure adequate organisation and may thus entail regulatory sanctions.65

In the area of competition law, the existence of compliance programmes to prevent contraventions of the CartA may provide a decisive argument to shield members of the governing bodies of an undertaking involved in unlawful conduct from personal criminal liability under Articles 54 and 55 CartA.

Valuable guidance for establishing a compliance programme in accordance with standards accepted as adequate by Swiss authorities may be found in ISO 19600 on compliance management systems, ISO 31000 on risk management and ISO 37001 on anti-bribery systems.66

---

59 Articles 44 et seq. FINMASA.
60 Articles 49 and 50 CartA.
61 Article 51 CartA.
62 Article 52 CartA.
63 Articles 54 et seq. CartA.
64 Article 102, Paragraph 2 CC.
iv Prosecution of individuals

As noted above, criminal law primarily addresses the conduct of individual perpetrators. Liability of undertakings is basically of an accessory nature only. Accordingly, criminal prosecution inevitably means prosecution of individuals, also in a corporate crime context.

To enhance the preventive effect of enforcement in the financial sector, FINMA has stepped up its action against individuals for suspected serious breaches of supervisory law since 2014.67 Consequently, action against individuals is an increasingly common feature of regulatory proceedings.68

Coordination of defence strategies and arguments between the undertaking and a targeted employee is often delicate as it may be perceived as collusion. In penal matters, supporting the defence of a suspected person by sharing information relating to the investigation, non-disclosure of relevant evidence, incomplete or misleading fact statements or the like may amount to unlawful assistance to evade prosecution.69 Furthermore, prosecuting authorities may, and often do, impose a duty of confidentiality on witnesses.70

Ideally, the undertaking therefore limits interaction with the targeted employee to obtaining information from him or her (or the employee’s counsel), whereas it cannot keep the employee apprised of its own strategies, actions and communications with the authorities.

During an investigation, an employee's contract should not be terminated. For as long as the employment relationship continues, the undertaking has a handle on the employee to assert compliance with directives and instructions and loyal safeguarding of the undertaking’s interests,71 which may include cooperation in fact finding and reporting on developments of concern to the employer.

While the undertaking may consider releasing the employee from his or her work pending the investigation (garden leave) for reputational reasons, or to avoid undue interference, it should not take disciplinary measures prior to completion of the investigation. Also, when considering any disciplinary measures, the undertaking must apply principles of fair process; the safeguarding of an employee’s personal rights (including the right to be heard) is mandatory.72 Regularly, undertakings concerned about criminal or administrative proceedings arrange for independent legal counsel to support the employee under investigation and sustain the resulting cost. As a rule, legal fees are paid by the employee only if he or she acted manifestly against internal regulations, instructions or statutory law.

67 FINMA guidelines on enforcement policy of 25 September 2014.
69 Article 305 CC.
70 Article 165 CPC.
71 Articles 321a and 321d CO.
72 See: Article 328, Paragraph 1 CO.
IV INTERNATIONAL

i Extraterritorial jurisdiction

There are several areas in which Switzerland imposes its laws and jurisdiction on undertakings (foreign or domestic) for conduct that took place outside Switzerland. This extraterritorial reach is often in line with obligations in international treaties and bodies of which Switzerland is a part, such as the United Nations, the European Convention on Human Rights and the OECD, and aims to safeguard against the infringement of human rights by corporations.73

In the public law domain, it is the Act against Unfair Competition,74 the CartA, the Data Protection Act and the Public Procurement Act75 that have extraterritorial reach. The competition law, for example, applies in all matters that have an unfair impact on the Swiss market irrespective of whether the infringing conduct took place within or outside Switzerland (effects doctrine).76 Similarly, competition law offences that have an effect in Switzerland can be investigated and sanctioned by COMCO even if they took place abroad.

Criminal law follows the principle of territoriality, but extends its reach with respect to certain offences. In the field of combating corruption in the private sector, Parliament recently introduced Articles 322-octies and 322-novies CC, which declare it punishable for anyone to offer or request undue advantages in exchange for carrying out or omitting an act in connection with the function in a company or organisation in the private sector, be it in contravention of duties or in the exercise of discretion. Active bribery in the private sector does not only expose the individuals committing the act to prosecution, but by virtue of Article 102, Paragraph 2 CC may also trigger the liability of the undertaking. This provision can lead to extraterritorial jurisdiction over non-domestic branch offices of Swiss undertakings.

A controversial initiative seeking to extend liability of Swiss undertakings to the conduct of entities abroad that are controlled by them, and to introduce mandatory governance standards based on the United Nations Guiding Principles on Business and Human Rights was debated extensively in Parliament.77 New legislation as a ‘counterproposal to the initiative’ will likely be put to the public vote together with the initiative. Should either of the proposed regulations become law, governance on undertakings and subsidiaries would be tightened and breaches by Swiss undertakings abroad would come within the reach of Swiss courts.

ii International cooperation

Switzerland cooperates with other countries’ government agencies, judiciary or prosecution authorities by way of administrative assistance or judicial assistance.78 The distinction of these two routes of cooperation is important. The Federal Supreme Court underlined that administrative assistance is limited to cooperation between administrative bodies and for administrative purposes (for example, the enforcement of tax laws) only, whereas information

74 Federal Act Against Unfair Competition (UCA, SR 241).
75 Federal Act on Public Procurement (SR 172.056.1).
76 Articles 3 and 7 UCA.
77 The initiative is known as ‘Konzernverantwortungsinitiative’; see: http://konzern-initiative.ch.
78 The Swiss government maintains a comprehensive database on the sources of law and forms relevant in international legal assistance, www.rhf.admin.ch/rhf/de/home/rechtshilfeuehrer/laenderindex.html.
required for the purposes of criminal prosecution must be sought by way of judicial assistance in criminal matters.79 There is no bypassing of the rules – and specific procedural guarantees – of judicial assistance by the route of administrative assistance.

Switzerland provides assistance in criminal matters that is not treaty-based under the International Mutual Legal Assistance Act (IMAC).80 There is no extradition of Swiss nationals against their will, but foreigners can be extradited under respective international treaties or the IMAC.81

FINMA cooperates with foreign supervisory authorities in specific supervisory or enforcement proceedings. The latest statistics (published in 2019)82 show a steady number of requests for international cooperation (436 in 2016, 457 in 2017, 340 in 2018) pertaining mostly to offences of insider trading, market manipulation and breach of reporting duties.

COMCO participates in a number of competition authority networks, such as the Competition Committee of the OECD and the International Competition Network. Bilateral and multilateral cooperation agreements exist between Switzerland and the European Union and other countries. The degree of integration allows for an efficient prosecution of anticompetitive cross-border activities.83

iii Local law considerations

There are certain criminal provisions that need to be considered in an investigation abroad having a nexus to Switzerland.

The first is the prohibition to carry out activities on behalf of a foreign state on Swiss territory without official approval, where the activities are the responsibility of a public authority or an official pursuant to Article 271 CC. This provision is intended to prevent the exercise of foreign official power on Swiss territory and thus protect state sovereignty. An act attributable to an authority or official is any act that characterises itself as such by its nature and purpose, regardless of whether it was carried out by a person formally holding an official position. The decisive factor is, therefore, not the individual, but the official character of the conduct. The Federal Supreme Court recently held that the disclosure of client information to US authorities by a Swiss-based asset management company with a view to facilitating the conclusion of a non-prosecution agreement violated Article 271 CC, despite the responsible manager of the company claiming he had not and could not have been aware that he was committing an unlawful act at the time of the relevant conduct.84 The criminal sanction may also apply to foreign attorneys travelling to Switzerland for the purpose of an investigation85 and may even cover the remote accessing of information via a Swiss-based server.

The second is the ban on divulging Swiss business secrets to foreign entities and states pursuant to Article 273 CC. A ‘Swiss business secret’ is any information of commercial value that is not in the public domain outside Switzerland and that typically relates to a business domiciled in Switzerland.86 It applies also to the intra-group and cross-border disclosure of

79 Federal Supreme Court judgment dated 28 December 2017, 2C_640/2016.
80 Federal Act on International Mutual Assistance in Criminal Matters (SR 351.1).
81 Article 32 of the International Mutual Legal Assistance Act.
82 See: www.finma.ch/de/durchsetzung/amtshilfe/internationale-amtshilfe/.
84 Federal Supreme Court Decision 6B_804/2018 of 4 December 2018.
86 id., p 361 n 29.
business secrets from a subsidiary to the parent company. Even the inadvertent cross-border disclosure of facts may constitute a violation of Swiss business secrecy. Further, Article 47 of the Banking Act sanctions the duty on banks to keep private information about their clients confidential (often referred to as bank secrecy). The purpose of the provision is to safeguard the privacy of the client; it is not a confidentiality privilege of the bank. The Federal Supreme Court recently ruled that Article 47 of the Banking Act does not apply to subsidiaries of Swiss banks abroad.\footnote{Federal Supreme Court Decision 6B_1318/2016 of 10 October 2018.}

Article 162 CC makes it an offence to reveal a business secret that has to be guarded pursuant to a statutory or contractual obligation.

In Swiss law, attorney–client privilege is expressly guaranteed by the Attorneys Act\footnote{Article 13 Federal Act on Free Movement of Attorneys (BGFA, SR 935.61).} and any breach is sanctioned by criminal law.\footnote{Article 321 CC: the person violating the professional secret may, upon complaint, be liable to a custodial sentence of up to three years or to a monetary penalty.} However, the concept of legal privilege is fairly narrow and does not (yet) encompass legal advice from in-house counsel or external legal experts who are not members of the Swiss Bar.\footnote{Whether and to what extent foreign lawyers can invoke legal advice or representation privilege widely depends on the rules applying in their own jurisdiction. Switzerland tends to recognise the core elements of foreign privilege rules.} A recent proposal for amendments to the Swiss Code on Civil Procedure contains a new Article 160a, which – if enacted – extends legal privilege to in-house counsel and their team for ‘attorney-specific’ work performed under the auspices of a person who attained a domestic bar registration or equivalent permit for attorney work.\footnote{See: www.bj.admin.ch/bj/de/home/staet/gesetzgebung/aenderung-zpo.html.}

\section*{V YEAR IN REVIEW}

In 2019, new developments in combatting money laundering were brought in. The Federal Supreme Court ruled with a view to cross-border matters that money laundering may only be committed on assets that are subject to forfeiture pursuant to the laws of the jurisdiction competent to prosecute the predicate offence.\footnote{Federal Supreme Court, judgment of 6 August 2019, BGE 145 IV 335.} The judgment clarified that money laundering as a criminal provision aims to protect the state’s interest of confiscation of proceeds of a crime as a means to re-establish legal order and to enforce, in particular, the principle that ‘crime must not pay’. If the applicable foreign statute provides no basis to confiscate the assets at issue, though such assets are the proceeds of a criminal act, no criminal liability for money laundering in the sense of Article 305-bis CC ensues.

MROS introduced a new electronic system for reporting suspicion of money laundering. The Swiss Federal Office of Police (Fedpol) signed a treaty with the United Nations Office on Drugs and Crime that will give it access to a programme used by Financial Intelligence Units worldwide and allows for efficient tracking and evaluation of financial transactions.

The OAG brought several large money laundering procedures to a close: one resulting in the forfeiture of more than 130 million Swiss francs and restitution of these assets to Usbekistan; another with a verdict against a banker who had assisted a former Greek government official in laundering corruption payments.\footnote{www.bundesanwaltschaft.ch/mpc/en/home/taetigkeitsberichte/taetigkeitsberichte-der-ba.html.} In the \textit{Petrobras-Odebrecht}
investigation, the OAG was able to restitute 400 million Swiss francs to Brazil. The 1MDB case remains ongoing, while some of the FIFA-related cases ended by expiry of the limitation period for prosecution. After some procedural setbacks, the hearings at the Federal Criminal Court had been set for March or April 2020, just as the covid-19 crisis was at a peak and the health situation of one of the accused did not permit attendance at a hearing.

The failure of the FIFA prosecution and irregularities surrounding the work of the OAG itself have shed an unfavourable light on the criminal prosecution system in Switzerland. Against the background of repeated infringements with governance rules by the Attorney General, including informal, unrecorded meetings with high-ranking representatives of FIFA that triggered the suspicion of partiality of the prosecution, the Supervisory Authority on the Office of the Attorney General (SA-OAG) opened a disciplinary investigation against the Attorney General on 9 May 2019. The findings and conclusions of the investigation were published on 4 March 2020.94 The SA-OAG found that the Attorney General, inter alia, had repeatedly made misleading and untrue statements about his meetings with FIFA officials, that he violated the OAG’s code of conduct on the avoidance of conflicts of interest and that he obstructed the investigation. While the Attorney General has appealed the verdict of the SA-OAG, public and political pressure on him to resign are growing.

The importance of transparency and the role of whistle-blowers in combatting corruption and crime is widely recognised. Yet, the National Council rejected the draft bill on the protection of whistle-blowers in the private sector and thus downed a legislative process that had lasted for years. As a result, Switzerland does still not have a comprehensive legal framework for whistle-blowers. Nevertheless, undertakings should implement procedures encouraging the reporting of irregularities and handle reports of perceived wrongdoing with care and diligence as a matter of diligent corporate governance. By doing so, corporates may not only strengthen their ability to prevent loss as a result of disloyal or unlawful conduct, but also protect themselves and their management from potential civil or even criminal liability for organisational deficiencies.

VI CONCLUSIONS AND OUTLOOK

Navigating an undertaking through criminal or administrative investigations remains a challenge, although case law has in recent years significantly sharpened the contours of best practice. A number of important issues are still pending clarification:

a Attorney–client privilege in connection with internal investigations: case law remains in flux as regards the prerequisites for, and scope of, protection of attorney work products in internal investigations. The proposed extension of legal privilege to in-house lawyers may bring clarification.

b Protection of whistle-blowers: the mutual rights, obligations and duties of individuals on the one hand and undertakings on the other will remain uncodified. In the absence of a specific legal framework, companies should take guidance in best practices that have evolved during the past years.

c Multi-jurisdictional investigations: the legal corset of domestic and international laws on administrative and judicial cooperation is often perceived by investigating authorities and – in some instances also by undertakings and individuals investigated – as not flexible enough to sensibly respond to the challenges of multi-jurisdictional

investigations; cooperation is thus often informal. Also, there continues to be a high
degree of uncertainty as regards protection of basic civil rights in matters that are being
investigated in parallel in various jurisdictions, such as nemo tenetur and ne bis in idem.
Protection of supervisory privilege: Swiss courts, including the Federal Supreme Court,
have in the past repeatedly confirmed the prosecutors’ authority to compel undertakings
and individuals in criminal investigations to disclose documents (including internal
investigation reports) that had been prepared for regulatory purposes even where the
competent regulatory agency expressly declined to share such documents with the
prosecuting authorities.

What remains clear, however, is the need for constant review and improvement of compliance
structures to keep pace with national and international developments. Adequate organisation
and, no less importantly, a culture promoting compliance, are the most efficient ways to
minimise exposure to criminal or regulatory scrutiny in general and the uncertainties outlined
in this chapter in particular.
INTRODUCTION

Public prosecutors and criminal courts are the primary authorised bodies to investigate and prosecute corporate conduct. In addition to public prosecutors and criminal courts, the Financial Crimes Investigation Board is also authorised to investigate crimes concerning money laundering, under the Law on the Prevention of Laundering of Crime Revenues. There are other regulatory authorities with significant powers to investigate corporate wrongdoings, within the scope of their regulatory and supervisory duties and powers. For example, the Turkish Competition Authority (the TCA) has the power to conduct dawn raids at companies and the Banking Regulation and Supervision Agency (the BRSA) has the power to conduct on-site examinations as per Article 14 of the Regulation on Procedures and Principles Regarding the BRSA’s Examinations. The Capital Markets Board has the authority to make on-site examinations upon the chairman of the Capital Markets Board’s request and an order made by a Criminal Judgeship pursuant to Article 90 of the Capital Market Law.

Although there is no legislation that imposes on companies an obligation to cooperate with these authorities during an investigation, such a cooperation would be beneficial for companies as there are sincere repentance provisions under the Turkish Penal Code (the TPC), which provide serious remissions for bribery, theft, abuse of trust and reckless bankruptcy crimes. These will be discussed in more detail in the following sections.

CONDUCT

i Self-reporting

Turkish law does not specifically set forth any reporting obligation for legal entities in case of any criminal offence. However, there is a general reporting obligation under the TPC. Accordingly, all individuals who have knowledge of a criminal offence that is still in progress or that has been committed, the consequences of which can potentially be avoided or at least limited, must report these offences to the Public Prosecutor’s Office. Failure to report such a

1 Fikret Sebilçoğlu is a partner at Cerebra CPAs & Advisors. Okan Demirkan is a partner and Begüm Biçer İlikay is a senior associate at Kolcuoğlu Demirkan Koçaklı.
2 Published in the Official Gazette dated 11 October 2006 and numbered 5549.
3 Published in the Official Gazette dated 22 July 2006 and numbered 26236.
4 Published in the Official Gazette dated 6 December 2012 and numbered 6362.
5 Published in the Official Gazette dated 12 October 2004 and numbered 25611.
criminal offence is punishable by imprisonment of up to one year. The Constitution provides an exception to the reporting obligation, stating that no one shall be compelled to make a statement that would incriminate himself or herself.

Additionally, employees have a loyalty obligation towards their employers under the Turkish Code of Obligations (the TCO). Accordingly, employees must act loyally to protect the righteous interest of their employers. By virtue of this loyalty obligation, employees should notify their employers about any unlawful circumstances that may harm the employers’ financial well-being and reputation. Even if the conditions for a general reporting obligation are not met, employees should report the issue internally in light of the loyalty and proportionality principles. If the issue cannot be addressed internally, then employees may turn to relevant public authorities.

Other legislative provisions that are related to self-reporting are the sincere repentance provisions regulated under the TPC. For instance, the TPC regulates that if an individual commits bribery, but then informs the authorities and returns the benefit gained as a result of the crime before the authorities become aware of the crime, this individual shall not be penalised for bribery. There are other sincere repentance regulations under the TPC regarding crimes such as theft, abuse of trust, bankruptcy by deception and reckless bankruptcy.

In addition to the above pieces of legislation, leniency programmes also play an important role in case of a possible self-reporting. The TCA established a leniency programme that rewards undertakings for self-reporting a cartel. The Regulation on Active Cooperation for Discovery of Cartels (the Leniency Regulation) sets out the main principles of granting immunity and leniency. The TCA also published the Guidelines regarding the Regulation to clarify the application of the leniency programme. According to the Leniency Regulation, the first undertaking to provide information and evidence regarding a cartel agreement may be granted full immunity from fines. An undertaking may apply for leniency until the TCA finalises its final report regarding the investigation.

ii Internal investigations

A company may conduct an internal investigation at its own initiative. There is generally no limitation for companies to initiate such internal investigations. During an internal investigation, hard copies and electronic documentary evidence, interview notes, expert reports issued by forensic accounting investigators and computer forensic professionals are commonly used. Although the composition of each internal investigation team may vary depending on the knowledge and skills required by the type of investigation, an internal investigation team generally includes management representatives, in-house and external lawyers, forensic accounting investigators, computer forensic experts and IT personnel. After the investigation process, the company will only be obliged to report the investigation's result to external bodies if the investigation is required by the court or any other regulatory body. However, the Capital Market Law sets forth a disclosure obligation in case of developments that may affect capital market instruments’ value.

In addition to the internal investigations, several institutions are also authorised to appoint their officers to conduct investigations on certain type of legal entities. The Ministry of Finance is one of these authorised institutions. Accordingly, within the framework of the

---

6 Published in the Official Gazette dated 4 February 2011 and numbered 27836.
7 Published in the Official Gazette dated 15 February 2009 and numbered 27142.
Law on the Prevention of Laundering of Crime Revenues, the Ministry of Finance may order its supervisory personnel to investigate banks, insurance agencies, private pension agencies and capital markets services.8

Another important legal issue during internal investigations is the attorney–client privilege. There are several provisions under Turkish law that broadly define related concepts on the protection of attorney–client privilege, but there is no legal regulation that expressly grants a legal professional privilege to attorney–client relationships. Article 36 of the Attorneyship Law9 sets forth a confidentiality obligation for any document or information that attorneys obtain while practising their profession and Article 130/2 of the Criminal Procedural Law10 (the CPL) provides that any material that is confiscated as part of a search conducted in an attorney’s office must be returned immediately to the attorney if the material is understood to relate to the professional relationship between a client and that attorney. In recent years, the TCA has evaluated attorney–client privilege in some of their decisions. One of the important decisions of the TCA is known as the CNR Decision.11 In this decision, the TCA underlines two main principles of the attorney-client privilege: (1) the correspondence should be between an external counsel (i.e., not an in-house counsel) and the relevant institution; and (2) the purpose of this document should be establishing a legal defence.

In another decision, the TCA concluded that a document including legal advice on how to cover up antitrust violations would not be subject to attorney–client privilege based on the justification that such document was not related to the exercise of the defence right.12 Following the TCA’s decision, the company filed an administrative lawsuit, requesting the decision’s cancellation. The administrative court held that this document’s purpose was to detect antitrust violations and to provide compliance solutions, thus concluded that this document was related to the exercise of the defence right and should be protected under the attorney–client privilege.13

In addition to internal investigations, under the Turkish Commercial Code (the TCC), upon a shareholder’s request companies may request from commercial courts the appointment of a special auditor to clarify certain events or doubts.14 There must be an affirmative general assembly resolution in order to request this appointment from commercial courts. If the general assembly resolution is not affirmative, then shareholders holding an aggregate of 10 per cent of the share capital (20 per cent in publicly listed companies), or shareholders whose aggregate shares’ value is at least 1 million Turkish lira may request the appointment of a special auditor from the commercial court. The competent commercial court will decide on the special audit’s subject within the framework of the request. The special audit’s results will be reported to the court and then to the company’s general assembly of shareholders.

---

8 Published in the Official Gazetted dated 11 October 2006 and numbered 26323.
9 Published in the Official Gazette dated 7 April 1969 and numbered 13168.
10 Published in the Official Gazette dated 17 March 2004 and numbered 25673.
11 The TCA Decision dated 13 October 2009 and numbered 09-46/1154-290 K.
12 The TCA Decision dated 6 December 2016 and numbered 16-42/686-314 K.
14 Published in the Official Gazetted dated 13 January 2011 and numbered 6102.
iii Whistle-blowers

Turkish Law does not provide any specific rule regarding whistle-blowing. Nonetheless, there are rights and obligations prescribed under Turkish law that may apply to whistle-blowing cases. One example would be Article 18(c) of the Labour Law, which specifically prohibits an employer from terminating an employment contract on the basis that the employee has filed a complaint or participated in proceedings against the employer seeking fulfilment of obligations or rights arising from the law or the employment contract.15

In addition, there are repentance provisions under the TPC that provide serious remissions for bribery, theft, abuse of trust and reckless bankruptcy crimes. The whistle-blowing concept not being regulated under the Capital Market Law is criticised in practice. Some lawyers argue that, because whistle-blowing would address many of the aims of corporate governance, the Capital Market Law and its secondary legislation should include incentives and protections for whistle-blowers.16

Due to lack of specific whistle-blowing regulation in Turkey, companies should consider general principles of legislation such as criminal, employment and data protection law when handling with whistle-blowing. Having said that, there is no restriction on private companies to adopt internal whistle-blowing regulations as part of their ethics and compliance policies and procedures.

A recent study by Karamanoğlu Mehmetbey University pointed out that when employees are exposed to an act that constitutes an ethical violation, employees who choose to remain silent tend to be the ones with the relatively lower levels of education. Conversely, employees with higher levels of education tend to be more active in whistle-blowing.17

III ENFORCEMENT

i Corporate liability

In principle, legal entities cannot be sentenced to imprisonment or a judicial fine. Only individuals can be punished. However, security measures such as cancellation of licences and confiscation of profits associated with the crime can be imposed on companies, if the representatives or authorised employees commit a crime for the benefit of the company and not for their personal benefits.

In principle, the same counsel may defend both the company and the suspected employee, unless there is a conflict of interest between the two. In practice, however, this is generally not advised, because in time the relations between the company and the employee may evolve into a conflict throughout the investigation or because of entirely unrelated factors. Article 38 of the Attorneyship Law regulates the conditions under which attorneys are obliged to reject an individual or legal entity’s request for representation. A conflict of interest is one of the conditions that require an attorney’s rejection. The Union of Turkish Bar Associations concluded in one of its decisions that an attorney representing a cooperative in a commercial lawsuit and then representing the cooperative’s chairman in a criminal lawsuit constituted a conflict of interest, because the chairman had allegedly committed

15 Published in the Official Gazette dated 10 June 2003 and numbered 25134.
embezzlement against the cooperative. However, the conditions that constitute a conflict of interest are not exhaustively listed under the Attorneyship Law and the presence of a conflict of interest will be evaluated on a case-by-case basis.

**ii Penalties**

In case of criminal proceedings because of a company’s transaction, courts can impose security measures on legal entities. The representatives, authorised bodies or third parties who perform a task within the framework of the company’s field of activity may also be subject to imprisonment or a judicial fine. The TPC provides that if a legal entity’s activities are subject to a permission granted by a public body and if this legal entity abuses its right arising from this permission, then the criminal court can decide on the permission’s withdrawal. It is also possible for the court to render a decision on the confiscation of the property or profits associated with the crime. There are certain conditions for the confiscation of a legal entity’s properties: (1) the crime must be committed with the participation of the bodies or representatives of the legal entity; (2) the crime must abuse the permission granted by the public body; and (3) the legal entity must benefit from the crime. Additionally, the imposed security measure must not have greater consequences than the committed crime (i.e., the penalty must be proportional).

In addition to the penalties regulated under the TPC, there are also administrative fine regulations under the Law on Misdemeanours. The Law on Misdemeanours provides that legal entities will be subject to administrative fines if crimes such as fraud or bribery are committed. The amount of the administrative fine will be between 10,000 and 2 million Turkish lira. The competent criminal court will decide on the fine’s amount, considering the concrete elements of the incident (e.g., the amount of the bribe and the benefit obtained by the relevant company as a result of this crime).

**iii Compliance programmes**

With the exception of banks and other financial services companies, there is no legal requirement under Turkish law for companies to have a compliance programme. However, the Regulation on the Programme of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism sets forth a compliance programme obligation for banks and other institutions such as capital market intermediary institutions and insurance companies. The board of directors will be responsible for the compliance programme’s implementation.

For other companies, although there is no legal requirement to adopt and implement a compliance programme, the existence of such a compliance programme may affect the authorities’ decision on the penalty amount in case of a crime committed by the company’s employees or representatives. For this reason as well as others, in practice Turkish companies are increasingly adopting and implementing their own compliance programmes. Any corporate compliance programme implemented by entities conducting activities in Turkey must adhere to Turkish laws. The National Profession Standards of Ethics and Compliance

---

18 Union of Turkish Bar Associations Decision dated 17 January 2015 and numbered 2014/615 E and 2015/47 K.
19 Published in the Official Gazette dated 31 March 2005 and numbered 25772.
20 These are the amounts applicable for 2020 and they are subject to a yearly amendment.
21 Published in the Official Gazette dated 16 September 2008 and numbered 26999.
Management Level 6 (the Standards) prepared by the Ethics and Reputation Society, a private sector-oriented association which guides its members and stakeholders all over Turkey to create their business ethics policies (TEID), regulate the standard working environments and conditions, tools and equipment to be used, measurement, evaluation and documentation systems. The Standards also address the roles and responsibilities of an ethics and compliance officer. Preparing ethics and compliance programmes, including policies and procedures, ensuring that the ethics and compliance programmes are implemented and organising ethics and compliance related training and awareness activities are among the ethics and compliance officer's responsibilities. TEID has not only prepared the Standards but also established certification programmes to train ethics and compliance officers. As of today, more than 130 ethics and compliance officers have received certificates after attending this programme. Although the Standards are not a legal requirement for private companies yet, ethics and compliance professionals believe that TEID’s efforts will increase awareness in organisations considering the heightened ethics and compliance risks particularly related to corruption, bribery and fraud.

iv Prosecution of individuals

There is no legal requirement to terminate an employee's contract because of or upon the results of an investigation process. However, it is possible to terminate an employee's contract with valid or just reason, or to cancel a manager’s authorities, depending on the investigation's outcome. Depending on the circumstances, the employer may also choose to terminate the employee’s contract because of strong suspicions of wrongdoing.

Another option is for the employer to remove the relevant employee from the workplace because of serious suspicion, without terminating his or her contract or cancelling his or her authorities, so that the employer can carry out the investigation and gather evidence in a more fertile environment. In such cases, what is generally known as ‘garden leave’ is implemented in practice (i.e., removing the employee from the workplace before the internal investigation begins or for as long as it continues). During this period, the employee continues to receive his or her employment entitlements but does not actively come to the workplace. The garden leave concept is not regulated under Turkish law. Although, in practice, an employee on garden leave does not physically go to the workplace, in theory it would be possible for the employee to go to the workplace as the garden leave is not legally regulated. In the absence of legislative provisions regarding garden leave, it would be beneficial to include this concept in employment contracts, in order to avoid complications.

IV INTERNATIONAL

i Extraterritorial jurisdiction

The TPC provides that if a Turkish citizen commits an offence in a foreign country that would constitute an offence subject to a penalty of imprisonment where the minimum limit is greater than one year under Turkish law, a penalty under Turkish law will also be imposed, provided that the relevant citizen has not been convicted for the same offence in the foreign country as well. Another regulation under the TPC concerns crimes committed by non-citizens. If a non-citizen commits an offence to the detriment of Turkey in a foreign
country, which would constitute an offence subject to a penalty of imprisonment where the minimum limit is greater than one year under Turkish law, and the relevant party is in Turkey, a penalty under Turkish law will be imposed. Furthermore, the TPC lists offences such as torture and intentional pollution of the environment as offences, to which Turkish law will apply regardless of where these crimes are committed and regardless of the offender’s citizenship.

In addition to the above, the TPC has provisions with extra-territorial effect regarding the crime of bribery. Accordingly, if: (1) public officials who have been appointed or elected in a foreign country; (2) officials working in international or foreign state courts; (3) members of international parliaments, individuals who perform a public duty for a foreign country; (4) citizens or foreign arbitrators who are appointed for a dispute resolution; and (5) officials or representatives of international organisations which have been established by international agreements commit the bribery crime, they will be punished according to the TPC.

### ii International cooperation

Turkey is keen to cooperate with other countries in areas that require international collaboration. A good example is the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. Turkey is party to this convention along with 32 other countries. The extra-territorial effect of the crime of bribery as regulated under the TPC is one of the successful implementations of this convention in Turkish legislation.

In addition to the aforementioned convention, Turkey has signed and ratified several conventions and mutual treaties with several countries regarding extradition. One of these treaties is the Third Additional Protocol to the European Convention on Extradition, signed by more than 30 countries. Turkey also has bilateral extradition treaties with the USA, Algeria, Morocco, Iraq, Iran, Kazakhstan, Kuwait, Turkish Republic of Northern Cyprus, Libya, Lebanon, Egypt, Mongolia, Uzbekistan, Pakistan, Syria, Tajikistan, Tunisia and Jordan.

### iii Local law considerations

Under Article 90 of the Constitution, duly ratified international agreements have the force of law. In this respect, if a bilateral or international treaty is in force, the provisions of that treaty become domestic law. In internal investigations, one significant concern is the use and maintenance of private data. Treaties generally have specific provisions on how to handle privileged information or private data, but in some cases, Turkey may reserve the right to request the relevant authorities’ (e.g., the BRSA, Personal Data Protection Agency) consent prior to sharing any sensitive data.

In large-scale investigations involving several jurisdictions, investigations are generally carried out locally in accordance with Turkish law and regulations. Exceptions may apply in cases involving national security or relating to Turkey’s diplomatic relations, in which case different rules may be applicable. In addition, should it prove necessary for the public prosecutor to obtain evidence abroad, he or she may request support from other countries’ authorities in accordance with the relevant multinational or bilateral treaty.

---


V YEAR IN REVIEW

Criminal investigations are conducted in a confidential manner in Turkey. For this reason, there is no publicly available official information on the details of recent criminal investigations. However, most practitioners would probably agree that in the last few years Turkey has seen significant improvements in the implementation of white-collar crime related penalties. In the past, Turkish courts were more reluctant to impose criminal penalties for many white-collar crimes, as they generally adopted the approach that commercial losses should be dealt with as commercial disputes and not criminal. This approach has been changing, thanks to several factors including the fact that prosecutors have become more inclined to indicting individuals for these crimes instead of categorically dismissing complaints for being ‘of a commercial nature’.

While prosecutors and courts are less reluctant to apply the TPC and penalise white-collar crimes in the private sector, unfortunately Turkey’s implementation of anti-corruption and anti-bribery laws in the public sector are not among the country’s strengths. In February 2020, Transparency International released its annual Corruption Perception Index. This year, with a score of 39, Turkey has dropped to the 91st place out of 180 countries. Compared to last year, Turkey dropped 13 places after losing two points.

Although there are efforts in recent years to bolster Turkey’s response to corruption, there continue to be significant challenges in implementing the range of laws intended to combat economic crime and corporate misconduct. Surveys indicate that establishing an effective whistle-blowing structure and implementing it properly are frequently among the biggest challenges for private companies in Turkey. This is mainly because of: (1) the corporate cultural and Turkish cultural perspectives having significant impact on responses of employees toward witnessed wrongdoings; (2) inherent difficulties in structuring objective and independent reporting roles and responsibilities with good governance; and (3) difficulties in managing the reported wrongdoings. In addition, the lack of whistle-blower laws designed to encourage individuals to raise concerns of misconduct or wrongdoing does not leverage efforts to foster whistle-blowing culture in private companies.

In investigations conducted in recent years, it is generally seen that clear, accurate and unbiased reports prepared by forensic accounting professionals and digital forensic experts have become more critical in the results of court cases. There is an increasing trend that these reports become extremely crucial elements in legal procedures, as they provide properly and legally obtained documentary evidence and interview notes derived from interviews with witnesses. Prosecutors generally take these reports seriously and more often than not they base their indictments on the findings highlighted in these reports.

VI CONCLUSIONS AND OUTLOOK

The developing international regulatory environment and extraterritorial anti-bribery laws such as the FCPA, UK Bribery Act and Sapin II have had significant impact on Turkish companies’ internal investigation policies and procedures. Increasing enforcement in several jurisdictions and particularly of the FCPA in the United States has resulted in increased risks of criminal and civil penalties for individuals and companies, who in Turkey are increasingly more aware of the possible consequences of these risks. This awareness has caused corporate scrutiny focusing on compliance issues, particularly compliance with local legal obligations as well as extraterritorial laws. With the OECD Corporate Governance Principles and Corporate
Governance Principles announced by Capital Markets Board of Turkey, Turkish companies have been encouraged to establish and ensure the effectiveness of compliance programmes to comply with applicable laws, regulations and standards.\(^{25}\)

Despite the lack of any regulation imposing a cooperation obligation on companies during an investigation, awareness regarding the importance of preventing white-collar crimes has been increasing day by day. Non-governmental organisations such as TEID and the Corporate Governance Association of Turkey as well as international institutions such as Transparency International have played significant roles in raising awareness on these matters. These institutions have been continuously organising workshops and conferences and have even published comprehensive guides on how to conduct internal investigations to prevent, detect and take action on wrongdoings.

I INTRODUCTION

The US government during the presidency of Donald J Trump has announced various incremental policy changes to its approach to corporate enforcement. These include the expansion of policies to decline corporate prosecutions for companies that sufficiently cooperate and self-report misconduct, adoption of an ‘anti-piling on’ policy towards penalties, changes in the prosecutorial focus on individuals, and issuance of new guidance for corporate compliance programmes and corporate monitorships. Despite these changes, however, there has been little evidence of a major shift in the sustained trend over the past decade of aggressive US criminal and regulatory enforcement activity against corporations and their directors, officers and employees. Eight-, nine- and even 10-figure monetary penalties continue to be the norm on a number of enforcement fronts, and aggressive investigations and prosecutions of individuals engaged in corporate misconduct remain common.

In the environmental law and consumer fraud arena, the fallout from the automobile emissions investigations continues. In 2017, Volkswagen reached an agreement with regulators requiring it to pay more than US$4 billion in criminal and civil penalties in connection with allegations that it sold cars with ‘defeat devices’ intended to circumvent emissions testing and environmental regulations. Several former Volkswagen executives and employees, including the former chief executive officer (CEO), were criminally charged for their role in the conspiracy, two of whom were sentenced in 2017 and are serving their terms of imprisonment in Germany; this was in keeping with the more aggressive stance by the Department of Justice (DOJ) in the years following the fallout from the 2007–2008 financial crisis in pursuing and obtaining guilty pleas from individuals implicated in corporate misconduct. In 2019, the DOJ and Attorney General of California reached a civil settlement in excess of US$500 million with Fiat Chrysler Automobiles (FCA) for similar conduct, and brought its first criminal charges against an Italian engineer for conspiracy, with other unnamed FCA employees, to mislead regulators. Reports indicate that criminal and civil authorities in the United States and abroad continue to investigate FCA and other automakers for potential violations of vehicle emissions rules.

In the financial sector, regulators continue actively to investigate currency, interest rate, futures market manipulation, and consumer protection issues. In June 2018, Société Générale entered into a deferred prosecution agreement with the DOJ and paid a US$275 million fine for manipulation of LIBOR. In April 2018, Wells Fargo was fined US$1 billion by the Bureau of Consumer Protection and the Office of the Comptroller of Currency for violations...
relating to the bank’s auto loan and mortgage practices; in December 2018, it agreed to pay US$575 million to resolve investigations by all 50 US states and the District of Columbia for a range of sales and other practices; and, in February 2020, Wells Fargo agreed with the DOJ and the US Securities and Exchange Commission (SEC) to pay US$3 billion to resolve potential criminal and civil liability stemming from a range of sales and other practices. In April 2020, Bank Hapoalim, Israel’s largest bank, reached a resolution concerning conspiracy to hide assets and income of US taxpayers in offshore accounts. Bank Hapoalim agreed to pay US$875 million and its Swiss subsidiary pled guilty under a deferred prosecution agreement (DPA) to conspiracy to defraud the United States.

In addition to obtaining guilty pleas and substantial monetary penalties from financial institutions, the DOJ has continued to pursue charges against individuals; for example, in October 2018, the DOJ secured a guilty verdict against two former Deutsche Bank derivatives traders on charges of conspiring to manipulate LIBOR; although in that same month, a federal jury acquitted three former foreign exchange traders from Barclays, Citigroup and JPMorgan of charges of conspiring to fix daily benchmark rates on foreign exchange spot markets. In November 2019, the DOJ obtained a conviction of a former JPMorgan currency trader after a three-week trial for price fixing and bid rigging. The DOJ has also continued with prosecutions of financial institutions and individual traders as part of its ‘spoofing takedown’ initiative announced in 2018. In June 2019, Merrill Lynch Commodities Inc agreed to pay US$25 million under a non-prosecution agreement for deceptive trade practices known as spoofing. In September 2019, the DOJ brought charges against individual JPMorgan traders for spoofing, which included a racketeering conspiracy charge under a statute traditionally used to prosecute criminal enterprises.

On the foreign bribery front, after a pause in the announcement of new settlements following the presidential transition, enforcement resumed at a rapid pace with the DOJ and SEC imposing approximately US$2.9 billion in penalties for violations of the Foreign Corrupt Practices Act of 1977 (FCPA) in 2018 and another approximately US$2.9 billion in 2019. Significantly, US regulators continued to target non-US companies and individuals suspected of anti-corruption violations, often with the cooperation of foreign governments and regulators. For example, the 2018 Petrobras anti-corruption settlement, which resulted in the imposition of more than US$1.78 billion in criminal fines, penalties and forfeiture, was the result of an investigation conducted jointly by authorities in the United States and Brazil. The 2018 US$585 million corruption settlement with Société Générale to resolve bribery allegations relating to improper payments in Libya was coordinated among US and French authorities, and the DOJ credited the bank with over US$292 million for payments made to French prosecutors to resolve the investigation. In March 2019, the US$850 million corruption settlement with Mobile Telesystems and its Uzbekistan-based subsidiary involved the assistances of law enforcement authorities in more than a dozen countries.2 In 2020, the US$3.9 billion settlement under a DPA with France-based aerospace company Airbus SE to resolve foreign bribery charges resulted from significant assistance by law enforcement from France and the UK, and the US$1.06 billion settlement under a DPA with Sweden-based Telefonaktiebolaget LM Ericsson and the guilty plea of its Egypt subsidiary for violating the FCPA involved significant assistance from law enforcement authorities in Sweden. While the DOJ and SEC have been responsible for some of the largest FCPA-related settlements to date

2 Austria, Belgium, Cyprus, France, Ireland, Isle of Man, Latvia, Luxembourg, Norway, the Netherlands, Switzerland, Sweden and the United Kingdom.
over the last few years, the US Commodity Futures Trading Commission (CFTC) announced in March 2019 its intention to bring enforcement actions in foreign corruption cases where the underlying conduct related to CFTC-regulated activities, such as commodities contracts. The CFTC advised, however, that it would not ‘pile on’ in imposing penalties imposed by other agencies and would, when imposing penalties for commodities-related violations of the FCPA, provide ‘dollar-for-dollar credit’ for disgorgement or restitution paid to other agencies.

The statutes authorising these prosecutions represent just a sliver of the interlocking regulatory and legal regimes in the United States, in which companies must comply with numerous regulations and statutes or face criminal or civil sanctions. There is no shortage of regulatory agencies empowered to take action in the event of a compliance lapse. The most prominent of these include the DOJ, the SEC, the Internal Revenue Service (IRS), the Environmental Protection Agency (EPA), the CFTC, the US Departments of Commerce, Labor and the Treasury, the Federal Energy Regulatory Commission, the Occupational Safety and Health Administration and banking regulators such as the Federal Reserve and the New York State Department of Financial Services (DFS). Many of these agencies are empowered to commence formal investigations and enforcement proceedings on their own initiative and impose monetary sanctions or other penalties.

Still, the DOJ – charged with prosecuting corporate crimes such as money laundering, bribery and tax fraud – is uniquely formidable among the agencies because of its power to indict and prosecute criminally, the threat of which has remained an important method of ensuring corporate compliance during the past decade. This was demonstrated not only by the passage of the 2002 Sarbanes–Oxley Act and the expansion of corporate criminal statutes, but also by the contemporaneous revision of the United States Sentencing Commission’s (USSC) Organizational Guidelines to impose harsher penalties for corporate malfeasance.

For large-scale corporate investigations and prosecutions, the DOJ frequently coordinates with other federal agencies, as well as state and local authorities. The 2017 Volkswagen settlement, for example, resulted from an investigation that was closely coordinated between the DOJ and the EPA. The DOJ has partnered with the Department of Health and Human Services to combat financial fraud in federal and state healthcare programmes, and announced, in September 2018, a US$260 million settlement with Health Management Associates for criminal and civil charges concerning overbilling government healthcare programmes and alleged kickbacks to physicians. And, in recent years, the DOJ has coordinated with the SEC and CFTC in spoofing enforcement. This coordination extends to interagency ‘task forces’, such as the establishment in July 2018 of a task force on market integrity and consumer fraud that, among other things, combats corporate fraud that victimises the general public and the government.

The DOJ has also pursued enforcement actions against a number of international financial institutions in recent years for the failure of anti-money laundering controls and for processing transactions on behalf of parties subject to US economic sanctions administered by the Office of Foreign Assets Control (OFAC) of the US Treasury Department.3 In late 2012, HSBC paid a then-record US$1.9 billion for failures in its anti-money laundering procedures.

---

programme and its own business with sanctioned parties; BNP Paribas paid a US$8.9 billion fine for similar conduct in 2014. In April 2019, Standard Chartered paid US$1.1 billion to US and UK authorities and UniCredit paid US$1.3 billion to US authorities to resolve investigations into their compliance with US sanctions laws. The DOJ has seldom filed criminal charges against international financial institutions outside of a settlement agreement, but in October 2019, the DOJ indicted Halkbank, the second-largest state-owned bank in Turkey, for helping Iran evade US sanctions in a criminal proceeding that Halkbank is contesting. The DOJ investigations in these actions have been conducted in conjunction with the New York County District Attorney’s Office, OFAC and the US bank regulatory agencies, in addition to global regulators such as the UK Financial Conduct Authority.

A corporation facing a criminal investigation by the DOJ or other agencies typically feels great pressure to avoid an indictment, which carries the risk of severe reputational, legal, regulatory and other ‘collateral’ consequences (even apart from the potential criminal penalties such as fines, forfeiture, disgorgement of unlawful profits and restitution). For many companies, particularly highly regulated ones, a mere indictment – before conviction or even after acquittal – can have severe reputational effects, and disastrous consequences for a company’s stock price and its ability to seek funding in the capital markets. Moreover, corporations in certain industries, such as companies that serve as government contractors for the Department of Defense or participate in the federal government’s Medicaid and Medicare programmes, can face crippling suspension upon the filing of charges and mandatory exclusion from the programmes if ultimately convicted. The collateral consequences of a corporate criminal investigation and prosecution may not be reversible even if the company is vindicated on appeal. For example, Arthur Andersen, an 89-year-old firm with 85,000 employees, implicated in the Enron accounting fraud, suffered severe damage to its reputation after being indicted by the DOJ and lost its licence to audit public companies after being convicted of felony obstruction of justice. Although that conviction was overturned in 2005 by the Supreme Court, the firm had already suffered irreparable harm and had by that time ceased to function as a viable business. It is therefore not surprising that most companies facing regulatory investigations cooperate as fully as possible in the hope of avoiding formal charges and frequently self-report potential wrongdoing in which the company or its employees may be implicated.

II CONDUCT

i Self-reporting

Most federal enforcement agencies4 have published official policies emphasising the importance of voluntary disclosure and full cooperation in an investigation, and pledging to take into account any disclosure or cooperation (or lack thereof) in determining whether to bring an enforcement action and what kind of penalties to seek. The USSC Organizational Guidelines also explicitly provide for reduced sentences for companies that provide ‘timely and thorough cooperation’, where ‘timely’ is defined as ‘begin[ning] essentially at the same time as the organisation is officially notified of a criminal investigation’.

4 Including the DOJ, the SEC, the EPA, the enforcement arms of the Treasury Department, Departments of Defense and Health and Human Services and the CFTC.
In some cases, the benefits of self-reporting and cooperation are unambiguous. The Department of Defense, for instance, will not pursue suspension or debarment sanctions against companies that self-report and cooperate, and the Antitrust Division of the DOJ offers full amnesty to the first company involved in an antitrust cartel that comes forward to voluntarily disclose its participation, makes restitution to victims of the cartel and cooperates in the investigation and prosecution of other culpable companies. The cooperating company’s directors, officers and employees will also receive amnesty if they are willing to cooperate in the investigation.

In most other settings, however, voluntary disclosure and cooperation are just two of many factors that regulators and prosecutors promise to ‘take into account’ in their charging calculus, without specific guidance as to how much weight each will be accorded in relation to other factors affecting the charging decision. For example, both the DOJ and the SEC have explicitly included voluntary disclosure and cooperation in their respective official enforcement policies, and in the DOJ and SEC’s 2012 FCPA resource guide, as factors to be weighed. High-ranking representatives from these agencies commonly make public pronouncements regarding the importance of voluntary disclosure and are quick to cite examples of companies that were purportedly spared severe sanctions after disclosing and cooperating fully. In spite of these assurances, it is difficult to isolate any quantifiable benefit that can be attributed to voluntary reporting as opposed to other factors because of the lack of visibility in the regulators’ decision-making process and the multitude of factors that affect both the decision to charge and the severity of the ultimate penalty imposed. Given the regulators’ clear interest in having companies come forward on their own initiative to disclose wrongdoing, thereby avoiding the burden of independently detecting illicit activity, companies may have good reason for some degree of scepticism of the professed benefits of self-disclosure.

In apparent response to criticism regarding the uncertain benefits of self-reporting and cooperation in the FCPA context, the DOJ implemented a pilot programme in April 2016 with the aim of providing additional guidance for prosecutors investigating FCPA violations and motivating companies to disclose potential FCPA violations. The pilot programme expanded upon prior DOJ guidance by articulating the specific requirements that companies must satisfy to be eligible for reductions in penalties as a result of voluntary disclosure, cooperation with the DOJ and remediation (i.e., the implementation of effective FCPA compliance controls) and quantifies the potential reduction in fines for which a qualifying company may be eligible: up to 50 per cent off the minimum USSC Organizational Guidelines range if the target company fully complies with the criteria set out in the announcement. In November 2017, the DOJ announced a new corporate enforcement policy intended to expand and replace the pilot programme. This includes a new presumption that the DOJ will decline to prosecute if a company satisfies the policy’s requirements for voluntary self-reporting, cooperation and timely remediation (though the company will still be required to disgorge any ill-gotten gains). In 2018, the DOJ announced that it was informally expanding this policy outside the FCPA context.

Since its pilot programme, the DOJ has made numerous revisions and clarifications that appear to greater incentivise companies to self-report. For example, in March 2019, the DOJ clarified that a company could still obtain the benefits of this policy even if ‘aggravating factors’, such as the involvement of senior management in the underlying misconduct, were present if the company’s actions were ‘otherwise exemplary’. In November 2019, the DOJ
clarified that companies are required only to disclose facts known ‘at the time of disclosure’ (as opposed to the prior ‘all relevant facts’ standard), and eliminated the requirement of companies to disclose certain evidence that a company ‘should be aware of’.

Even with this additional guidance from the DOJ, it is not completely clear that voluntary reporting should be the default action of every company that discovers potentially unlawful conduct within its organisation. A company must, of course, first determine whether it has a mandatory legal obligation to disclose potential wrongdoing that it discovers. For example, financial institutions may be obliged to report suspicious activity. Sarbanes–Oxley also imposes numerous compulsory reporting requirements on companies should they discover certain types of fraud and other misconduct. Because many of the regulators have information-sharing agreements or otherwise coordinate their actions, if a company decides to self-report, it may be prudent to make the disclosures to all agencies with jurisdiction in order to receive the maximum potential self-reporting credit. Even without a mandatory legal obligation, a company should at the very least assess the probability of independent discovery of the potential misconduct by government authorities. The likelihood that a government agency will independently become aware of an impropriety has increased significantly in recent years as a result of the general upturn in regulatory enforcement activity, the expansion of international cooperation, the proliferation of new laws and regulations favourable to whistle-blowers, and the development and adoption of sophisticated technology to detect potential misconduct.

In determining whether to self-report, and to what extent to cooperate with a regulatory investigation, corporations and their employees must also bear in mind that should they be deemed to be impeding or obstructing the investigation, in addition to charges relating to the conduct under investigation, they may potentially face charges of obstruction of justice or conspiracy to commit obstruction of justice. These charges are typically much easier to prove than charges stemming from the underlying conduct being investigated and can carry penalties that are equally, or more, severe. Under Sarbanes–Oxley, for example, an individual can face up to 20 years in prison for altering or falsifying documents with the intention of obliterating a federal investigation and a company can face substantial fines for this conduct. In recent years, the DOJ has not hesitated to seek such penalties against companies and employees that are perceived to be uncooperative or evasive, and the SEC and other agencies have been known to refer reports of obstructive conduct during civil enforcement actions to the DOJ for criminal prosecution. For instance, in February 2018, Rabobank agreed to forfeit US$369 million and pleaded guilty to obstructing an investigation into deficiencies in the bank’s anti-money laundering compliance programme conducted by Rabobank’s primary regulator, the Office of the Comptroller of the Currency of the US Treasury Department.

ii Internal investigations

In conjunction with disclosing potentially improper conduct to the government, a corporation will typically undertake an internal investigation, either on its own initiative or with the encouragement of the relevant government agency, to determine whether unlawful activity has in fact occurred and, if so, which employees are responsible. There are several important reasons for conducting such an investigation. First, a full understanding of the facts can be crucial to mounting a defence in any adversarial proceedings that might arise with government authorities or in any private civil suits that might be filed. Second, by conducting an internal investigation and disclosing important information gleaned from a review of documents and employee witness interviews to federal agencies, a corporation may
be more likely to receive credit for cooperation and thereby decrease its risk of indictment and the imposition of severe penalties. Finally, simply as a matter of good corporate governance, it is important for the corporation to be confident that it has accurately determined which employees were responsible for the unlawful activity and to ensure that it has implemented adequate controls to prevent any recurrence of the wrongdoing.

Even if a company has not yet made the decision to report potentially unlawful conduct to a regulator, it still might have cause to conduct an internal investigation after, for example, (1) receiving a tip about fraudulent activity on a dedicated company hotline, (2) receiving information from an internal or external auditor about a potential compliance issue or (3) being named in a civil suit by a former employee containing allegations of improper conduct on the part of the company. Further, because Sarbanes–Oxley requires companies to implement systems for the reporting of complaints by employees relating to accounting or auditing matters, and to conduct investigations in response to a wide range of concerns, companies are more likely than ever before to encounter situations in which the prudent course of action is to initiate an internal investigation.

It is generally advisable to have counsel supervise such investigations because of the likelihood that legal questions and issues will arise, although whether it is necessary to retain an outside law firm will depend on the company’s assessment of various considerations. In-house counsel may have the advantage of a more intimate understanding of the company’s operations and culture, while external counsel may have more experience conducting internal investigations and dealing with government agencies. In-house counsel’s familiarity with the company, however, can also be a weakness if it is perceived by the government to undermine objectivity, in which case the company may have more credibility in interacting with the government if it retains reputable external counsel. This is especially likely to be the case if any members of the company’s legal department are implicated in the conduct under investigation.

With respect to conducting these investigations, typically there are two primary components: review and analysis of relevant documents, and interviews with company employees who have knowledge of the relevant facts. Generally, documents are gathered and reviewed prior to conducting interviews, which allows the interviewer to focus on key issues or questions discovered during the course of the document review, or to seek clarification on potentially inculpatory or troubling statements contained in those documents. At the outset of each interview, the standard practice is to notify the employee that the attorney conducting the interview is counsel to the company and not the interviewee’s personal attorney, and that while the conversation is protected by attorney–client privilege, that privilege belongs to the company, which it may waive at its sole discretion. The employee should also be informed that any information imparted during the interview may be shared with government authorities.

Unless it uncovers nothing to merit any disclosure during the course of the internal investigation, a company will typically present its findings to the government after completing the document review and interviewing process, or – for a particularly complex investigation – at the conclusion of some segment of that process. Those presentations can be made orally or in written form, in response to which the government may identify additional areas of concern that require follow-up work. The government and counsel may then engage in dialogue regarding whether criminal or civil charges are warranted – and what kind – and how much credit to give to the company for its cooperation. In making its case for leniency, it may be effective for a company to argue not only that the facts uncovered do not amount to actionable misconduct, but also, from a policy perspective, that the relevant agency’s objectives would not be advanced by pursuing an enforcement action against the company.
company should also consider reviewing the agency’s published charging guidelines (such as the DOJ’s guidelines for the prosecution of business organisations) to support an argument that an enforcement action is not warranted or that the situation calls for reduced charges; for example, by emphasising (1) that senior management was not implicated in the wrongdoing and, therefore, the misconduct was not pervasive, (2) that the company has no history of related misconduct, (3) that the company had an robust and effective compliance programme in place at the time of the offence or (4) that the collateral consequences of enforcement would be unjustifiably severe.

Whether conducted by in-house or outside counsel, a significant amount of attorney–client privileged information and attorney work-product material will be generated during the course of an internal investigation. Prior to 2006, the DOJ expected that a corporation would waive attorney–client privilege and provide all requested materials and information if the company wished to be given credit for cooperation. There was significant criticism of this policy from the corporate sector, the defence bar and various members of Congress. In response, the DOJ revised its policy in 2008 and now categorically directs prosecutors not to seek a waiver of privilege and prohibits prosecutors from taking waiver into account when making a cooperation determination. The current policy does, however, allow prosecutors to consider the extent to which the company has disclosed all ‘relevant facts’. Therefore, despite the government’s assurances that waiver is not necessary to obtain credit for cooperation, a company may find that it is not possible to make a full disclosure of the ‘relevant facts’ without turning over privileged materials. Other agencies, such as the SEC, have published similar policies, and in recent years, some courts have held that oral summaries of witness interviews offered by companies to regulators as part of their cooperation constituted a waiver of the attorney–client privilege and attorney work-product protections over interview notes and memoranda prepared by company counsel.

iii Whistle-blowers

The probability of a US company facing a whistle-blower complaint increased significantly with the implementation of the whistle-blower provisions of Dodd–Frank, which came into effect in 2011. Under Dodd–Frank, the SEC must award whistle-blowers who alert the SEC to certain types of wrongdoing that result in successful enforcement actions rewards of between 10 and 30 per cent of the total monetary sanctions collected by the SEC over US$1 million. The new whistle-blower rules expand the already far-reaching protections for whistle-blowers created by Sarbanes–Oxley and the False Claims Act, including extending Sarbanes–Oxley whistle-blower coverage to employees of non-public subsidiaries of publicly traded companies. According to its 2019 annual report to Congress on the programme, the SEC has received more than 33,300 tips since it was introduced in August 2011. For the first time since its introduction, in fiscal year 2019, the SEC saw a marginal decrease of about 1 per cent in the number of tips, which suggests a levelling off of whistle-blower complaints. The programme has resulted in SEC actions yielding more than US$2 billion in total monetary sanctions. The SEC has paid several substantial bounties to whistle-blowers who have given information leading to successful prosecutions. As of 2019, the SEC had awarded US$387 million to 67 individuals, including its largest award in 2018 of more than US$50 million to two whistle-blowers who jointly provided information leading to a successful enforcement action.

Given this complex regulatory regime, a company must proceed with even greater caution when confronted with allegations of misconduct by a whistle-blower. Any credible
tips describing potential illegal acts should be investigated promptly and thoroughly, with the assistance of outside counsel if necessary. If the company determines that the allegations have merit, it should take swift remedial action and consider self-reporting its findings to interested regulators. By no means should a company take any action that might be perceived as retaliation against the whistle-blower, as such behaviour could potentially expose the company to substantial civil or criminal liability. In 2017, the CFTC amended its whistle-blower programme rules to strengthen protection for corporate whistle-blowers. The SEC continues to take aggressive action against companies perceived to be taking adverse action against whistle-blowers or attempting to frustrate or interfere with their protection and rights. For example, in 2017, the SEC fined the financial services company HomeStreet, Inc US$500,000 for attempting to uncover the identity of a whistle-blower after being contacted by the SEC in connection with an investigation and for including provisions in severance agreements with former employees causing those employees to waive severance payments if they receive a whistle-blower award. In June 2018, the SEC announced proposed amendments to its whistle-blower program. While many of its proposals further incentivised reporting by whistle-blowers, the amendments also proposed a discretionary US$30 million cap on awards.

III  ENFORCEMENT

i  Corporate liability

Because of the way in which the doctrines of corporate criminal and civil liability have evolved in the United States, prosecutors and regulatory agencies have considerable leverage over business organisations. Generally speaking, companies are liable for the actions of employees if the employees’ conduct is ‘within the scope of their employment’ and they act at least in part with ‘the motive of benefiting the company’. These two qualifiers have been interpreted to place little meaningful limit on a company’s potential exposure. For example, corporations have been held liable where the wrongdoing at issue benefited only the employee and was perpetrated in violation of the company’s explicit instructions. Moreover, it is irrelevant where the culpable employee falls on the corporate ladder; legally speaking, the conduct of a post room clerk is imputed to the company to the same extent as the company’s CEO. Further, under the collective liability or collective scienter doctrine, a company may be liable – particularly in the civil context – if its employees, when considered in the aggregate, possessed sufficient knowledge and intent to violate the law, even if no single employee had the requisite mental state or corrupt intent. Some courts have limited the application of this doctrine in recent years. Notably, in February 2020, a US court overturned a jury conviction of a former Alstom SA executive on foreign bribery charges after finding that prosecutors had failed to prove that the executive was an ‘agent’ of the company’s US subsidiary. Nevertheless, the doctrine can still be an attractive option for a regulator bringing, for example, a complex securities fraud case against a huge, decentralised company.

ii  Penalties

Regulators have a vast arsenal of potential sanctions to impose on corporations convicted of a statutory violation. Among other potential penalties and sanctions, various regulatory statutes authorise criminal or civil fines (or both), restitution, disgorgement, criminal
forfeiture, probation and community service. Further, as mentioned above, the collateral consequences of a conviction can be just as damaging, potentially resulting in suspension or debarment from eligibility for government contracts, reputational harm and a drop in the company stock price. Moreover, corporate investigations often involve multiple regulators with overlapping jurisdiction, raising the possibility that the corporation will face substantial penalties imposed by numerous authorities for the same underlying misconduct. Responding to concerns about ‘unfair duplicative penalties’, informally referred to as ‘piling on’, in May 2018, the DOJ announced a new policy encouraging coordination by the DOJ with other US and international law enforcement agencies conducting investigations of the same conduct to avoid ‘disproportionate enforcement of laws by multiple authorities’. Although the full impact of this policy has yet to be seen, there have been some signs in recent settlements that the DOJ is taking steps to reduce ‘piling on’, such as the June 2018 Société Générale settlement described above and the April 2019 Standard Chartered settlement in which the DOJ agreed to credit US$240 million for payments made to various US and UK authorities.

In the past, most corporate criminal investigations have ended with the two sides entering into a DPA or non-prosecution agreement (NPA), although there has been a marked increase in guilty pleas to resolve DOJ actions in more recent years. The typical DPA provides that the agency will file formal charges, which will be stayed for a period of time (usually between one and three years), after which the charges will be dismissed if the company has complied with certain obligations. These obligations typically require the company to: cooperate fully with the agency’s investigation and in any other investigation that may be ongoing; accept responsibility for the wrongdoing at issue; and undertake remedial action, including terminating or disciplining culpable employees, implementing revised internal controls and procedures and, in some cases, appointing an independent compliance monitor. The company also normally agrees to a monetary penalty, including a criminal or civil fine, forfeiture, restitution or disgorgement of unlawful profits. NPAs require similar types of performance on the part of the company but do not involve the formal filing of charges with a court. In both types of agreement, because the company has admitted to the conduct at issue (which is typically set forth in an agreed ‘statement of facts’ attached to the agreement), if a company is indicted upon breach of the agreement, conviction is almost certain. Previously, DPAs and NPAs were the exclusive domain of the DOJ, but the SEC has also recently adopted their use.

### Compliance programmes

Not only do DPAs typically require the implementation of an effective compliance programme or the improvement of an existing one, the existence of an effective compliance programme is also a factor that the DOJ and other regulators take into account in making their charging decisions. In 2017, the SEC’s ability to obtain disgorgement suffered a setback when the US Supreme Court held that a five-year statute of limitations applies to the imposition of disgorgement in SEC proceedings. The SEC has calculated that the decision led the SEC to forego seeking approximately US$800 million in potential disgorgement in filed and settled cases, with that amount expected to rise over time. In June 2020, the US Supreme Court upheld the SEC’s authority to seek and obtain disgorgement for a securities law violation in civil enforcement actions, but curtailed its scope so as to not exceed a wrongdoer’s net profits or its awards to victims.
decisions and may lead to a reduced sentence, in some cases up to 95 per cent, under the USSC Organizational Guidelines. The Guidelines provide guidance on the characteristics of a compliance programme that will be looked upon favourably by the government, which include:

- management that is knowledgeable about and able to oversee the programme competently;
- adequate staffing of the programme;
- training for all employees in compliance standards and procedures;
- procedures for monitoring and periodic auditing of the programme’s effectiveness;
- a system for the anonymous or confidential reporting of compliance breaches;
- consistent enforcement of the programme; and
- procedures for taking ‘reasonable steps’ to prevent further wrongful conduct if any is detected.

In 2010, the USSC revised its commentary to note that as part of the ‘reasonable steps’ to prevent the recurrence of wrongful conduct, a company should pay restitution to any victims that can be identified. The USSC further stated that the hiring of an ‘outside professional adviser’ to oversee the implementation of the compliance programme could also be considered a ‘reasonable step’. This led to speculation that the hiring of an outside consultant by the company may vitiate the need to impose an independent compliance monitor on a company as part of a regulatory settlement.

In recent years, there has been a trend towards self-monitoring and reporting rather than the imposition of an independent monitor as a standard feature of a settlement agreement. While there appeared to be a resurgence of the imposition of outside monitors in 2016, when regulators imposed eight independent compliance monitors in connection with FCPA settlements, the DOJ did not require any monitors in 2017 as part of its three FCPA resolutions. In April 2020, the DOJ published for the first time a list identifying all active corporate monitors by companies as part of criminal resolutions.6

Recently, the DOJ has moved to increase transparency in corporate criminal enforcements. In October 2018, the DOJ announced guidance setting forth factors the DOJ will evaluate in determining whether to impose a compliance monitor as part of a settlement with a corporation. These factors focus on the nature of the misconduct, the extent and effectiveness of the corporation’s remediation and the potential monetary costs and burdens on the corporation’s operations. In April 2019, and further updated in June 2020, the DOJ published extensive guidance on the factors it will consider in evaluating a corporate compliance programme in connection with determining the appropriate charging decision or form of resolution, the amount of monetary penalty and whether to impose a compliance monitor or other compliance obligations on a company. The guidance sets forth numerous examples of questions that prosecutors could ask a company in order to understand three ‘fundamental’ issues: whether the company’s compliance programme is well-designed, whether it is being implemented ‘earnestly and in good faith’ and whether it works ‘in practice’.

---

Prosecution of individuals

The question often arises during the course of a regulatory investigation of whether it is appropriate for a corporation to enter into a joint defence agreement with employees who are also under investigation. The DOJ’s official position is that the government may not consider such an arrangement in determining whether a corporation has cooperated with the investigation. However, as with the issue of waiver of privilege, the DOJ has qualified this position by noting that to the extent that such an agreement limits the company’s ability to disclose ‘relevant facts’, it may adversely affect the ability of the company to obtain credit for cooperation. Moreover, because various agency policies and the USSC Organizational Guidelines encourage corporations to cooperate fully in the prosecution of employees accused of wrongdoing, in many situations the risk of a conflict of interest between the company and its employees may preclude the possibility of entering into a joint defence agreement.

Conflicts of interest are more likely than ever to arise as, in the years following the 2007–08 financial crisis, the government became increasingly aggressive in pursuing individuals suspected of corporate malfeasance, and the DOJ has publicly announced that it favours prosecution of individuals over entities where feasible. For example, in October 2015, the DOJ issued the ‘Yates Memo’, which calls for more focus on individual defendants by prosecutors, states that credit for cooperation by companies will henceforth be contingent on disclosing ‘all relevant facts’ regarding individuals in the misconduct and prohibits the resolution of any corporate action without a ‘clear plan to resolve related individual actions’.

In 2018, the DOJ, under a new administration, relaxed the requirements of the Yates Memo to some extent, clarifying that a company may be eligible for at least partial cooperation credit if it makes good faith efforts to identify individuals ‘substantially involved’ in misconduct, even if the corporation is unable to identify ‘all relevant facts’ about individual misconduct. Notwithstanding this change, the DOJ is unlikely to reduce its focus on individual prosecution, especially given numerous public comments by DOJ officials emphasising individual accountability for corporate crimes. Indeed, in 2019, the DOJ increased the number of indictments for FCPA-related violations to 34 individuals, up from 31 individuals in 2018 and 24 individuals in 2017.

IV INTERNATIONAL

Extraterritorial jurisdiction

Now more than ever, federal agencies are taking an expansive view of their statutory jurisdiction and aggressively pursuing foreign companies for violations of domestic law. Over the past decade, there has been an increase in the enforcement of US laws against corporate conduct that takes place largely outside the United States. This trend in ‘cross-border investigations’ is evident in a variety of contexts. For example, in November 2018, the DOJ announced its ‘China Initiative’, which concerns countering perceived national security threats to the United States from China by investigating and prosecuting Chinese companies for alleged trade secrets theft, economic espionage and other violations of US law.

In the FCPA context, a significant number of enforcement actions during the past few years – including many of the higher-value settlements – targeted foreign companies and individuals. While the FCPA applied only to issuers of stock on a US exchange when originally enacted, the statute now proscribes corrupt payments by any person, natural or otherwise, where relevant acts occur ‘in the territory of the United States’. Regulators have at times pushed the boundaries of this language, asserting jurisdiction, for example, based on
the fact that a transaction at issue was cleared through a US bank, even though no employee of the target entity took any action while physically present in the United States. Moreover, even where that minimum territorial connection is not met, the government has not hesitated to stretch traditional legal doctrines to assert jurisdiction; for example, by charging a foreign subsidiary with ‘aiding and abetting’ a violation by its US parent or for making an improper payment as the ‘agent’ of a US company. In 2018, a US appeals court rejected the DOJ’s attempt to employ theories of conspiracy or complicity to prosecute a foreign national, Lawrence Hoskins, who neither lived nor engaged in any alleged conduct in the US, for violating the FCPA. In November 2019, in a closely watched trial, a jury convicted Hoskins of violating the ‘substantive’ FCPA. The judge overturned the FCPA convictions in February 2020, finding that Hoskins was not an agent of a US entity and thus lacked sufficient territorial connection to be prosecuted under the FCPA. While a small number of court decisions, such as Hoskins, have pushed back on the regulators’ most aggressive attempts to extend jurisdiction, the significant expense and risk associated with litigating an FCPA action has resulted in few FCPA cases reaching the courtroom and therefore few legal or practical constraints on the extraterritorial reach of the FCPA.

Other countries have begun to look beyond their shores to target illegal conduct by corporations. For example, while previously criticised for its inaction in the foreign corruption arena, the United Kingdom enacted enhanced anti-bribery laws that came into effect in 2011. The law has an expansive jurisdictional scope that may exceed even that of the FCPA, theoretically allowing the UK government to assert jurisdiction over any company that does business in the United Kingdom, even if the conduct at issue occurred elsewhere. In 2012, UK authorities reaffirmed their commitment to aggressively pursuing criminal charges against suspected violators of UK anti-bribery laws, revising previously issued guidance on the laws that called for leniency or the imposition of civil fines only in certain situations. Recently, a number of other countries, such as Argentina, Brazil, France, Mexico, South Korea and Vietnam, have also expanded their anti-corruption, anti-bribery laws.

ii International cooperation

Because a successful international prosecution depends on effective cross-border cooperation and access to witnesses and evidence located abroad, the government frequently enlists the assistance of foreign governments and agencies in investigations. The DOJ, for instance, has many formal and informal relationships with foreign agencies to facilitate cross-border enforcement. Other agencies have not shied away from international investigation either; the SEC, for example, maintains an Office of International Affairs, through which it coordinates with foreign governments and provides training to foreign agencies in financial fraud enforcement. In 2017, the DOJ announced that it intended to continue its anti-corruption cooperation efforts with the United Kingdom’s Financial Conduct Authority and Serious Fraud Office by assigning a US prosecutor to those offices for a two-year term, after which the prosecutor will return to the United States to provide training and propose new policies based on his or her experience. Indeed, many of the highest-profile settlements have been the result of cooperative efforts between US and foreign regulators. For example, in January 2020,
Airbus SE, a France-based aerospace company, agreed to pay approximately US$4 billion in combined penalties – a record-high penalty – to the US, France and UK for violations of the FCPA. Indeed, the 10 largest FCPA settlements with the US were the result of cooperative investigations between US and foreign authorities.\(^9\)

### iii Local law considerations

Not all countries, however, have been as amenable to the expanding extraterritoriality of US law enforcement and enhanced cooperation among foreign authorities. Certain countries, including Mexico, Canada and some members of the European Union, have enacted ‘blocking statutes’ that prohibit, or place limits on, the production of information for use in a legal proceeding in a foreign country. This puts companies operating in the international arena in a difficult position, as compliance with one law may necessarily mean running afoul of another.

A multinational company under investigation by multiple regulators in other countries also faces innumerable complexities in dealing with varying and potentially inconsistent laws relating to the discovery of evidence and examination of witnesses. For example, data privacy laws in one country may prohibit the company from complying with a subpoena from a regulator in another, and the rights to counsel and against self-incrimination may be limited or absent under other regimes. This issue came to a head in 2017 in the form of a showdown between Microsoft Corp and the DOJ. The latter sought customer emails stored on a Microsoft server in Dublin pursuant to a warrant, and the former sought to quash the warrant on the basis, among others, that Microsoft would run afoul of foreign data privacy rules by complying. The case reached the US Supreme Court before it was dismissed in light of new legislation passed by Congress affecting the extraterritorial reach of US law enforcement requests, but the issue is likely to arise again in the near future.

### V CONCLUSIONS AND OUTLOOK

For at least the past decade, corporate and civil liability in the United States has moved inexorably towards more regulation and enforcement, harsher penalties and expanding jurisdiction. The Trump Administration, nearing the end of its term, has provided no obvious indicator of a reversal or suspension of this trend, at least in the short term, even in areas of enforcement considered by observers to be potential candidates for diminished activity, such as the anti-corruption front. The significant number of ongoing investigations, coupled with public comments by the DOJ and the SEC, also provide support for the proposition that a softening of corporate enforcement is not in the cards, despite recent policy adjustments by the DOJ that are intended to clarify or rationalise the process of resolving corporate investigations but that are unlikely to change underlying trends.

And while traditional areas of enforcement, such as anti-corruption, financial fraud and healthcare fraud, are likely to remain the mainstays of regulatory action, a number of other areas have emerged over the past few years and are likely to receive substantially increased focus going forward. Most prominent among these is cybersecurity – encompassing issues relating to data security, privacy, hacking, cryptocurrencies and related technologies and trade

---

\(^9\) These are: Odebrecht SA (US$3.56 billion), Airbus SE (US$2.09 billion), Petroleo Brasileiro SA (US$1.79 billion), Telefonaktiebolaget LM Ericsson (US$1.06 billion), Telia Company AB (US$965.6 million), Mobile Telecom Ltd (US$850.0 million), Siemens Aktiengesellschaft (US$800.0 million), VimpelCom Ltd (US$795.3 million), Alstom SA (US$772.3 million) and Société Générale SA (US$858.6 million).
secrets – all of which present significant regulatory challenges. The SEC, for example, formed a ‘cyber unit’ that has pursued a number of enforcement actions targeting the unregistered offering of cryptocurrencies, misconduct relating to abuse of financial markets through hacking, and the failure of public companies to timely disclose data breaches, and the SEC has also begun to announce policies and guidance designed to protect cryptocurrency investors. The DOJ launched its ‘China Initiative’ that has focused, among other things, on 5G technology, including corporate prosecution of the Chinese telecommunications conglomerate Huawei Technologies. While the ramifications of these new enforcement fronts remain unclear and will play out over the next several years, they will undoubtedly present compliance challenges for corporate actors.

What remains as clear as ever is the necessity of maintaining a robust compliance structure to promptly detect potential wrongdoing. While total prevention is unlikely, given the innumerable ways in which a company can run afoul of the law and the sheer complexity of the various regulatory regimes, prompt detection, thorough investigation and meaningful remedial action will limit the company’s exposure and maximise its chance of avoiding criminal or civil charges, or – failing that – negotiating a favourable settlement with government authorities.
Appendix 1

ABOUT THE AUTHORS

STUART ALFORD QC

Latham & Watkins

Stuart Alford QC is a partner of Latham & Watkins and former co-chair of the firm’s litigation and trial department in London. Mr Alford specialises in economic crime and regulatory matters, in particular for financial institutions, large corporates and high-growth companies. Much of his work involves multiple jurisdictions and cross-border issues of investigation and competing laws.

From 2012 to 2016, Mr Alford was head of the fraud division at the Serious Fraud Office (SFO), where he was responsible for many of the UK’s landmark white-collar cases. His work focused on investigations in banking and money markets, including the wide-ranging cases involving the manipulation of LIBOR, foreign-exchange benchmarks, and the Bank of England’s liquidity auctions.

Mr Alford has extensive experience engaging with law enforcement and regulators around the world, including, in particular, the UK Financial Conduct Authority and the US Department of Justice. Mr Alford has significant experience managing parallel criminal and civil litigation and has overseen significant data analysis projects and the advances in technology-assisted review and disclosure.

Before joining the SFO, Mr Alford spent 20 years in private practice as a barrister in London working in national and international criminal law. He was appointed Queen’s Counsel in 2014.

ILIAS G ANAGNOSTOPOULOS

Anagnostopoulos

Ilias G Anagnostopoulos has appeared as lead counsel in most of the significant corporate and criminal cases in Greece during the past 30 years and is a professor of criminal law and criminal procedure at the School of Law, National University of Athens. He has extensive experience in most types of business crime, financial fraud, European criminal law, tax and customs fraud, medical malpractice, product criminal liability, environmental liability, compliance, money laundering, corruption practices, anticompetitive practices and cartel offences, anti-terrorism, extradition and mutual assistance. His many publications in Greek, English and German deal with matters of Hellenic, European and international criminal law, business and financial crimes, reform of criminal procedure and human rights.
He is chair of the Hellenic Criminal Bar Association and a member of the Criminal Law Experts Commission (Ministry of Justice), the High-Legal Council with the Bank of Greece, and FraudNet of the International Chamber of Commerce.

RYOTA ASAKURA

Momo-o, Matsuo & Namba

Ryota Asakura is an associate at Momo-o, Matsuo & Namba. Mr Asakura routinely represents clients in litigation concerning corporate malfeasance and has extensive experience in internal investigations, especially as a member of internal investigation committees. His expertise covers all aspects of corporate scandals. Mr Asakura's corporate transactional practice is wide-ranging and includes mergers and acquisitions and, in particular, effective due diligence of acquisition targets. He also has broad experience in general corporate law matters including CSR and compliance having served as seconded in-house counsel to a global manufacturing company.

Mr Asakura is also expert in the field of administrative law and serves as a member of the Japan Law Foundation's study group on administrative lawsuits.

He received his LLB from the University of Tokyo, Faculty of Law in 2013 and was admitted to the Japanese Bar in 2015.

FERNANDO FELIPE BASCH

Bruchou, Fernández Madero & Lombardi

Fernando Basch specialises in corporate criminal law and corporate governance and compliance. He advises companies and international organisations such as the World Bank, the Inter-American Development Bank, the United Nations Development Programme, the World Economic Forum’s Partnering Against Corruption Initiative (PACI) and the Maritime Anti-Corruption Network (MACN). Fernando led the collective remediation strategy for MACN in Argentina, which reduced by 90 per cent the illegal solicitation to bulk carriers in Argentina. Who's Who Legal 2018 recognised his excellence as an expert consultant and recognised his expertise in criminal and anti-corruption law.

Fernando is also a senior researcher of the Centre for Anti-corruption Studies and associate professor on the LLM course in corporate law at the University of San Andrés. Moreover, he teaches economic criminal law on the LLM course at the Palermo University. He was also a visiting scholar at the Southwestern University School of Law (US).

Previously, Mr Basch was adviser to the Chamber of Deputies (2002–2006), director of the justice reform programme of Argentina’s Association for Civil Rights (ADC) (2009–2011) and secretary of the human rights programme of the National General Defender’s Office (2011–2012). He is a member of the Bar Association of the Federal Capital (Colegio Público de Abogados de la Capital Federal). He received his law degree from the Law School of the University of Buenos Aires (2001), completed a postgraduate degree in Criminal Law from the Palermo University (2005), and an MA in legal and political theory from University College London (2008). He also obtained an Anti-Bribery Specialist Accreditation (TRACE International, 2012).
SARAH BENZIDI

Linklaters LLP

Sarah Benzidi specialises in domestic and cross-border litigation and arbitration. Her areas of expertise include corporate disputes, white-collar crime, competition (including market practices) and consumer protection litigation.

ANUJ BERRY

Shardul Amarchand Mangaldas & Co

Anuj Berry is a partner with the firm’s litigation, dispute resolution and white-collar defence group. Anuj specialises in all issues of national and international white-collar crime, fraud, corruption and regulatory enforcement investigations. He has experience in both internal investigations and investigations by federal anti-corruption and anti-money laundering authorities. Anuj has represented multinational corporations in large and politically sensitive anti-corruption and anti-money laundering investigations having a cross-border element. His work involves assisting clients and senior management in all aspects of the investigation, guiding defence strategy and representation before courts or in investigations before regulatory and government bodies. He also assists in internal training and advises on the area of white-collar crime, both for management and personnel. Anuj has contributed articles to several global publications.

BEGÜM BİÇER İLİKAY

Kolcuoğlu Demirkan Koçaklı

Begüm Biçer İlikay is a senior associate at KDK. She has significant experience in dispute resolution and investigations. She represents domestic and international clients before Turkish courts and other public authorities in a wide range of litigation matters including commercial disputes, employment related disputes, administrative lawsuits, enforcement lawsuits and criminal proceedings in relation to white-collar crimes. Begüm is experienced in advising on the compliance of clients’ business practices with local and international anti-corruption and anti-bribery regulations and conducting internal investigations in relation to allegations regarding compliance matters. She was involved in several major investigation processes.

ALEXANDRE BISCH

Debevoise & Plimpton LLP

Alexandre Bisch is an international counsel in the Paris office of Debevoise & Plimpton LLP. He is a member of the Paris Bar and has experience in criminal and administrative investigations, as well as complex litigation, in France. He served for three years in the enforcement division of the French financial markets authority.

NICOLAS BOURTIN

Sullivan & Cromwell LLP

Nicolas Bourtin is a litigation partner at Sullivan & Cromwell LLP, co-head of the firm’s FCPA and anti-corruption group and the managing partner of the firm’s criminal defence and investigations group. His practice focuses on white-collar criminal defence and internal investigations, regulatory enforcement matters, class-action defence, and securities and

© 2020 Law Business Research Ltd
complex civil litigation. Mr Bourtin has conducted numerous jury trials and has argued frequently before the US Court of Appeals for the Second Circuit. He regularly represents companies and individuals under investigation by the US Department of Justice, the Securities and Exchange Commission, FINRA and other self-regulatory organisations, and state and local prosecutors’ offices. He has extensive experience in representing clients located outside the United States in defending against cross-border enforcement investigations.

From 2001 until 2005, Mr Bourtin served as an assistant US attorney in the Criminal Division of the US Attorney's Office for the Eastern District of New York. Mr Bourtin serves, on a pro bono basis, on the Criminal Justice Act panel for the Eastern District of New York. Mr Bourtin received his undergraduate degree magna cum laude from the University of Notre Dame and is a graduate of Columbia Law School, where he was a Harlan Fiske Stone scholar.

NATALIE BUTCHER

BDO LLP

Natalie is a director in the Forensic Technology team; a part of BDO’s Forensic Services practice in London. She has spent approximately 16 years in the forensic technology and eDisclosure fields, having graduated with honours with a BSc degree in Information Technology, Business Management and Language. Natalie is a fellow of the Association of Chartered Certified Accountants; the global professional accounting body.

Natalie has worked on a significant number of large eDisclosure projects throughout all areas of the process, from data scoping and collection right through to production and trial support. She is an expert in handling complex disclosures and is also experienced in data analytics. Natalie has worked directly with corporate clients in addition to their legal advisers and government bodies including the Securities and Exchange Commission, the Financial Conduct Authority and the Competition and Markets Authority. She has worked on many multijurisdictional cases and where mobile laboratories have been implemented due to strict data protection rules.

PEDRO LUÍS DE ALMEIDA CAMARGO

Siqueira Castro Advogados

Pedro Luís de Almeida Camargo holds a bachelor’s degree from University of São Paulo, is an associate at Siqueira Castro Advogados’ Corporate Criminal Law Department and has five years of experience with white-collar crime handling complex litigations and investigations, including corruption, tax, environmental, financial and money laundering cases.

ASMINA CEIC

Nyman Gibson Miralis

Jasmina Ceic is an accomplished criminal trial advocate. She advises and acts in complex criminal law matters at all levels of the court system, with a specialist focus on serious matters that proceed to trial in the superior courts, as well as conviction and sentence appeals heard in the Court of Criminal Appeal. She has represented and advised persons and companies being investigated for white-collar and corporate crime, complex international fraud and transnational money laundering.
JASON CHAN  
*Allen & Gledhill LLP*

Jason is a Senior Counsel and the Co-Head of the Firm's White Collar & Investigations Practice. He focuses on commercial litigation and international arbitration. He regularly advises local and overseas corporations on regulatory and white-collar criminal compliance matters, including market misconduct, corporate fraud and corruption. He also advises on corporate investigations and inquiries relating to regulatory and white-collar criminal compliance issues.

Prior to joining Allen & Gledhill, Jason was an Assistant Registrar at the Supreme Court of Singapore. Prior to that, he had served as a Deputy Public Prosecutor and State Counsel in the Attorney-General’s Chambers of Singapore, and as a Justices’ Law Clerk in the Supreme Court of Singapore.

Jason graduated from the National University of Singapore with an LLB (Hons) degree (First Class) in 2002. In 2009, on an academic scholarship, he obtained an LLM from Columbia University in the City of New York.

Jason serves as a member of several committees of the Singapore Academy of Law, including the Law Reform Committee. In 2008, he was admitted as an Advocate and Solicitor of the Supreme Court of Singapore.

KYLE J CHOI  
*Shin & Kim*

Kyle Choi is a senior foreign attorney at Shin & Kim and his major practice areas include cross-border intellectual property litigation including patents, trade marks, trade secrets, and product liability. Mr Choi joined Shin & Kim in 2019 having worked in US-based global law firms. Mr Choi obtained his Juris Doctor (magna cum laude) at the Catholic University of America, Columbus School of Law and is a member of the District of Columbia (Washington DC) Bar.

SEONG-JIN CHOI  
*Shin & Kim*

Seong-Jin Choi is a partner at Shin & Kim and his practice areas include corporate crime, high-tech crime, financial crime, money laundering, intellectual property rights and personal information protection. Starting his career as a prosecutor in 1997, Mr Choi has been in charge of many special investigations, including investigations against politicians and large corporations. While working as the digital forensic science officer at the Supreme Prosecutors’ Office, he gained vast experience in information technology-related crimes. He also worked as a directing manager at the South Korea financial intelligence unit of the Financial Services Commission.

JOÃO LIMA CLUNY  
*Morais Leitão, Galvão Teles, Soares da Silva & Associados*

João Lima Cluny joined Morais Leitão in 2007. He is a member of the firm’s criminal and compliance team. His practice focuses on the assistance of clients in the context of
criminal and regulatory offences and particularly in economic and financial domain. João has been involved in high-profile litigation cases in Portugal and has extensive trial experience, especially regarding corporate liability.

In recent years, João has been intensely working on matters related to compliance (regarding the prevention of corruption and money laundering), internal investigations and regulatory enforcement in different sectors such as sports, energy, competition, environment, banking, capital markets, labour, tax and media.

He is also a member of the arbitration, sport and entertainment, and infrastructure teams.

He is a member of the first instance club licensing body for UEFA competition of the Portuguese Football Federation and a member of the certification jury for the recognition, validation and certification process of professional competences of football coaches, nominated by the Portuguese Football Federation. He is also president of the Justice Council of the Portuguese Bridge Federation.

João Lima Cluny is an arbitrator and mediator of the Portuguese Court of Arbitration for Sports.

On the academic circuit, he holds a master’s degree in Forensic Sciences at the Nova Law School, where, since 2014, he teaches as Guest Professor (Interdisciplinary Legal Practice). He regularly participates in seminars and conferences predominantly on Criminal Law and Criminal Procedure, Arbitration and Sport’s Law. He is an author and co-author of articles on the same matters.

FREDERICK T DAVIS
Debevoise & Plimpton LLP

Frederick T Davis is a retired partner in the Paris and New York offices of Debevoise & Plimpton LLP. After serving as an Assistant United States Attorney in New York, he was in private practice in New York until 2006 when he moved to France and became a member of the Paris Bar. He is also a lecturer in law at Columbia Law School, where he teaches courses on comparative criminal procedures and cross-border criminal investigations. He is a life member of the American Law Institute and an elected Fellow of the American College of Trial Lawyers, and was named a chevalier of the National Order of Merit of France. In 2019 the Cambridge University Press published his book, American Criminal Justice: An Introduction.

OKAN DEMİRKAN
Kolcuoğlu Demirkan Koçaklı

Okan Demirkan leads KDK’s dispute resolution, energy and infrastructure, and ethics and compliance practices. He is a prominent figure in the area of ethics and compliance. He has conducted several investigations related to various regulatory as well as anti-bribery and anti-corruption allegations. He is an active board member of the Turkish Ethics and Reputation Society (TEID), Turkey’s leading civil society institution in the area of anti-corruption and ethics, of which KDK is a corporate member. Okan represents domestic and international clients in a wide range of litigation matters, including commercial disputes, employment related disputes, intellectual property claims, administrative disputes, enforcement and set-aside lawsuits at all levels of Turkish courts. He has particular expertise in criminal proceedings in relation to white-collar crimes. With significant experience of
almost 20 years in international arbitration, he regularly serves as counsel, arbitrator or expert witness in various commercial disputes involving Turkish law. In *Who’s Who Legal* 2019 and 2020, Okan has been recognised as a ‘Future Leader of the Arbitration World’ in Turkey.

**ULF DJURBERG**

*Setterwalls Advokbyrå AB*

Ulf Djurberg is head of Setterwalls’ EU and competition law department, which includes specialist groups on anti-corruption and special investigations, antitrust, merger control, public procurement, state aid, regulatory, trade and administrative law. Ulf has considerable experience in disputes in these areas and has been counsel in cases before Swedish national courts and the Court of Justice of the European Union. Ulf has also worked with worldwide antitrust and anti-corruption investigations.

Ulf regularly lectures at international conferences and symposiums.

**CIARA DUNNY**

*Matheson*

Ciara Dunny is a senior associate in the regulatory and investigations team within the commercial litigation and dispute resolution department. She has extensive experience in corporate crime and investigations and regularly advises both domestic and international clients on bribery, corruption, fraud, money laundering, investigations and trade sanctions, along with related compliance issues. Ciara’s experience in investigations extends to the United Kingdom, the United States, Europe, China, Korea, the United Arab Emirates and Iran.

**PHILLIP GIBSON**

*Nyman Gibson Miralis*

Phillip Gibson is one of Australia’s leading criminal defence lawyers with more than 30 years of experience in all areas of criminal law. Phillip manages and advises on the most complex criminal cases. Phillip has vast experience in transnational cases across multiple jurisdictions often involving assets forfeiture, money laundering and proceeds of crime, cybercrime, extradition, mutual assistance, white-collar crime, royal commissions, bribery and corruption, Interpol notices, international and national security law, and matters related to the Independent Commission Against Corruption and the Crime Commission.

**TAK-KYUN HONG**

*Shin & Kim*

Tak-Kyun Hong is a partner at Shin & Kim and his areas of practice include white-collar crime, anti-corruption and competition. Mr Hong has carried out a number of corporate criminal investigations and litigations. Prior to joining Shin & Kim in 2007, Mr Hong spent four years as a public prosecutor in South Korea. He is a *Chambers Asia* leading individual for dispute resolution (White-Collar Crime, 2015–2020), *Legal 500* Recommended Lawyer for Regulatory Compliance and Investigations (2019), and expert for investigations by *Who’s Who Legal* (2016–2017).
STEVE A HSIEH  
*Sullivan & Cromwell LLP*  
Steve A Hsieh is an associate at Sullivan & Cromwell LLP. He has experience in a broad range of matters, including internal and government agency investigations brought by the DOJ, SEC, EPA, and other regulators, as well as intellectual-property litigation, in federal court. Mr Hsieh received his undergraduate degree from the Georgia Institute of Technology and his law degree from the New York University School of Law.

THOMAS JENKINS  
*Debevoise & Plimpton LLP*  
Thomas Jenkins is an associate in the London office of Debevoise & Plimpton. He has extensive experience conducting anti-corruption investigations. He has advised clients facing a wide range of white-collar and regulatory defence challenges, including working on preventative measures and ongoing regulatory compliance. He has advised on a number of high-profile investigations involving a range of regulatory authorities. These have covered a variety of areas, from allegations of market abuse to allegations of worldwide supply chain corruption.

GUILLERMO JORGE  
*Bruchou, Fernández Madero & Lombardi*  
Mr Jorge received a law degree from the Law School of the University of Buenos Aires in 1995 and completed an LLM from Harvard University (2003).  
Mr Jorge is in charge of the compliance, investigations and corporate criminal law department.  
He is a recognised expert in anti-corruption compliance and money laundering prevention, and for his innovative strategies for mitigating legal risks.  
Prior to joining Bruchou, he was the founding partner of Governance Latam. Apart from advising multinational and local companies, he is regularly consulted in public reform processes, anticorruption and laundering prevention in Argentina and most Latin American countries, as well as by international organisations such as the World Bank, the Inter-American Development Bank, the United Nations and the Organization for Economic Co-operation and Development (OECD). He was also a member of FIFA’s Independent Governance Committee, which oversaw the organisation’s corporate governance reforms. *Who’s Who Legal* recognised him as a Global Elite Thought Leader in 2018.  
Additionally, he serves as a Global Adjunct Professor at the New York University School of Law and senior researcher at the University of San Andrés in the Centre of Anticorruption Studies. He has been a Visiting Scholar at the Center for Latin American Studies at Stanford University (2001), a scholar at the National Endowment for Democracy (2006) and at the Center for Democracy, Development and the Rule of Law at Stanford University (2009). He has published on the topics in which he specialises in Argentina and abroad and is a frequent speaker at international conferences. He is a member of the Bar Association of the Federal Capital.  
Furthermore, he has been recognised in his field of practice as leading lawyer by *Chambers and Partners*. 
NISHANT JOSHI  
*Shardul Amarchand Mangaldas & Co*

Nishant Joshi is a partner in the firm’s litigation and corporate group. He has been with the firm for over 17 years and has a total experience of over 20 years. Nishant has appeared in various courts and tribunals in India with regard to matters relating to white-collar crime, such as frauds, cheating, misappropriation, and breach of trust, money laundering, data theft, cybercrimes, defamation and other economic offences. He has conducted trials of complex criminal cases both as counsel for the complainant and assisting the prosecution and counsel for the accused. He has also handled cases under the Negotiable Instruments Act, FEMA, the Prevention of Money Laundering Act and the IT Act, etc., as well as conducting internal investigations for various clients. Nishant has also authored and co-authored articles and chapters in various publications on anti-corruption laws in India and has conducted training sessions for several companies in relation to compliance with Indian law. He has also rendered opinions and detailed memorandums on queries relating to criminal procedures, anti-corruption laws, anti-bribery laws, cyber laws and the Indian Penal Code.

ANTOINE KIRRY  
*Debevoise & Plimpton LLP*

Antoine Kirry is a partner in the Paris office of Debevoise & Plimpton LLP and heads the litigation practice of that office. He is a member of the New York Bar and the Paris Bar, and has extensive experience in criminal and administrative investigations, and complex litigation in France.

RONJA KLEISER  
*Setterwalls Advokatbyrå AB*

Ronja Kleiser is a member of Setterwall’s EU and competition law practice group, which includes specialist groups on anti-corruption and internal investigations, antitrust, merger control, public procurement, state aid, regulatory, trade and administrative law. Ronja has extensive experience in anti-corruption work and internal investigations within the private and public sectors.

TOMASZ KONOPKA  
*Sołtysiński Kawecki & Szlęzak*

Tomasz Konopka joined Sołtysiński Kawecki & Szlęzak in 2002. Since 2013, as a partner in the business crime and investigation team, he has led a team of lawyers (which he created in 2008) dealing with business crime cases. Before joining SK&S, he was an attorney for a number of years and sat on the boards of a range of firms, including those listed on the Warsaw Stock Exchange. He advises and represents clients in cases involving criminal liability risk. He advises entities that have incurred damage as a result of business crimes. He has extensive experience in conducting internal clarification proceedings, covering abuses such as corruption, fraud, money laundering, acting to the detriment of business entities, forgery and other crisis situations. He advises clients in planning and implementing comprehensive
compliance projects, as well as solutions that improve business security, including cybersecurity. He represents Polish and foreign clients before courts and prosecution authorities in Poland and abroad.

VICTOR LABATE

Siqueira Castro Advogados

Victor Labate holds a Bachelor of Laws from University of São Paulo (USP) and has also participated on the undergraduate exchange programme with Erasmus University Rotterdam (EUR), Netherlands, for criminology studies, having been awarded with an academic merit scholarship from USP.

He is an associate at Siqueira Castro Advogados’ Corporate Criminal Law Department and head of the office’s Car Wash Task Force, working mainly in cases of corruption, bid rigging and money laundering, counselling companies regarding possible risks of exposition and gathering evidences in internal investigations for later use in collaboration and leniency agreements.

VINCENT LEOW

Allen & Gledhill LLP

Vincent’s practice focuses on banking, employment, and shareholder disputes, as well as contentious investigations and inquiries. He has substantial experience in acting for banking and financial institutions, major corporates, and regulators on complex contentious matters. He also regularly advises clients on regulatory and risk management issues.

Vincent is consistently recognised for his expertise in several leading publications. The Legal 500 Asia Pacific recommends him as a ‘Leading Individual’ and describes Vincent as ‘one of the market leaders’, ‘very experienced in dispute resolution in the financial sector’, ‘highly experienced’, and ‘impresses with the quality of his work’. Similarly, he is described in Benchmark Litigation Asia Pacific as ‘building a reputation for [his] work in the commercial and transactions space’ and ‘highly commercial and provides very good service’.

Vincent serves on the faculty of the Singapore Institute of Directors (since 2015) and an advocacy trainer and facilitator at the Singapore Institute of Legal Education (since 2004). Vincent has been involved in various law reform reports, and has published articles in various law journals and contributed chapters to numerous leading practitioner texts, including the Singapore Civil Procedure 2020, and the Halsbury’s Laws of Singapore – volume 4 (Civil Procedure 2016).

JACKY LI

Global Law Office

Jacky Li is a partner based in the Shanghai office. He mainly focuses on regulatory compliance, internal and government investigation, competition laws, healthcare, dispute resolution, and labour and employment. Mr Li is well versed in conducting investigations in connection with anti-corruption (Chinese criminal and administrative law and US FCPA), anti-trust, white-collar crimes (embezzlement, financial fraud, insider trading, infringement of trade secret, etc.), data and cybersecurity from both Chinese and foreign law perspectives,
helping multi-national and state-owned enterprises to identify potential wrong-doers, assessing parameters of potential liability, and interacting with multi-jurisdiction government authorities.

Mr Li routinely advises clients regarding operational risk assessments and the establishment of internal control and compliance mechanisms. Prior to joining Global Law Office, Mr Li was a senior detective at the Shanghai Municipal Public Security Bureau, where he obtained extensive judicial experience and practical first-hand knowledge of criminal investigations and administrative enforcement, as well as the formulation of regulations and policies. When advising clients, Mr Li draws on this experience to ensure that his analysis includes the perspective of law enforcement agencies.

Mr Li has been ranked as a ‘next generation lawyer’ and ‘rising star’ in regulatory compliance practice by Legal 500 in 2019 and 2020, and has also been noted as a ‘recommended lawyer’ in healthcare practice by Legal 500 in 2019.

STEFAAN LOOSVELD

Linklaters LLP

Stefaan Loosveld specialises in litigation (including white-collar crime), contentious regulatory and restructuring and insolvency (including sovereign default and debt restructuring). He has worked in the firm’s New York and London offices. He acts for both financial institutions active throughout the eurozone and for corporates in complex litigation and arbitration matters.

Stefaan is the author of the book Money, Monetary Claims and Foreign Exchange in a Belgian, European and International Perspective and of numerous articles on topics related to finance and restructuring.

BERNHARD LÖTSCHER

CMS von Erlach Poncet Ltd

Bernhard Lötscher’s main practice areas are international mutual assistance in administrative, civil and criminal matters and advising an international corporate clientele on issues of criminal law and investigations. His professional experience also encompasses general contract, banking and financial services law. He is a member of the CMS dispute resolution practice group, the CMS anti-bribery and corruption practice group, and the banking and finance practice group.

Bernhard Lötscher has been a partner at CMS since 2001, heading the firm’s white-collar crime team.

GABRIEL LOZANO

Bruchou, Fernández Madero & Lombardi

Gabriel Lozano is a partner in the general corporate and M&A department of the firm and leads the firm’s competition and antitrust law department. His practice focuses primarily on mergers and acquisitions, and competition and antitrust law.

Prior to joining the firm, Mr Lozano was the General Counsel of Syngenta in LAS (Argentina, Chile, Bolivia, Paraguay and Uruguay) from 2015 to 2018. In this position, he played a major role in the acquisition of Syngenta by ChemChina and in the acquisition of
About the Authors

Nidera by Syngenta, both particularly focused on antitrust. In addition, in his daily practice he provided legal advice in contentious matters, contracts, data protection, trademarks and patents, and labour and regulatory law.

In 2020, Gabriel was elected President of the Competition Defense Commission of the Buenos Aires City Bar Association.

Mr Lozano received his law degree from the Law School of the University of Buenos Aires in 1998 and holds a postgraduate degree in International Business from Fundação Getulio Vargas (San Pablo, Brazil).

MARKUS MACHAN

wkk law Rechtsanwälte

Markus Machan is an attorney at wkk law Rechtsanwälte. Markus specialises in corruption and white-collar crime cases and advises clients in financial criminal matters and extradition proceedings. He graduated from the University of Vienna in 2009 and worked as a research assistant in the Department of Criminal Law at the University of Vienna from 2011 to 2014 and as research assistant at the Supreme Court of Justice. Markus Machan is a certified compliance officer, a lecturer at the University of Vienna and St Pölten University of Applied Sciences, a member of the Association of Austrian Defence Lawyers (VÖStV) and author of numerous specialist publications.

TIAGO COELHO MAGALHÃES

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Tiago Coelho Magalhães joined Morais Leitão in 2016. He is a member of the firm’s litigation team. His practice is mainly focused on criminal litigation and regulatory offences, as well as on matters concerning compliance. He previously worked with the firm’s European and competition law team.

PAULA MARTINEZ-BARROS

De Pedraza Abogados

Paula Martínez-Barros graduated in law from Complutense University of Madrid (2008) and has been a member of the Madrid Bar Association since 2009.

Before joining De Pedraza Abogados (October 2015), she worked for several years at the international law firm Baker & McKenzie in the area of white-collar crime and corporate compliance. She holds a master’s degree in business administration (MBA) from University of San Diego (California, 2015), specialising in corporate finance and international business. She completed a semester exchange programme at SDA Bocconi School of Management in Milan, and two ‘compliance officer’ expert programmes from Thomson-Aranzadi (2016).

With business and law studies behind her, Ms Martínez-Barros now specialises in white-collar crime, the implementation of corporate compliance programmes of national and multinational companies and conducting internal investigations (at national and international level).
Vanessa McAllister
*wwk law Rechtsanwälte*

Vanessa McAllister is partner at wkk law Rechtsanwälte and responsible for the wkk law branch office in Salzburg, Austria, that has been set up in January 2020. Vanessa graduated from the University of Salzburg in 2013 and worked as a research assistant in the Department of Criminal Law at the University of Salzburg from 2013 to 2016. Her doctoral thesis, published in 2017, deals with criminal aspects of the cartel law fine. She is a member of the Association of Austrian Defence Lawyers (VÖStV) and author of numerous specialist publications.

Dennis Miralis
*Nyman Gibson Miralis*

Dennis Miralis is a leading Australian defence lawyer who acts and advises in complex domestic and international criminal law matters in the following areas: white-collar and corporate crime, money laundering, serious fraud, cybercrime, international asset forfeiture, international proceeds of crime law, bribery and corruption law, transnational crime law, extradition law, mutual assistance in criminal law matters, anti-terrorism law, national security law, criminal intelligence law and encryption law. He appears in all courts throughout Australia and regularly travels outside Australia for complex international and transnational criminal law matters.

Wynne Mok
*Slaughter and May*

Wynne Mok is a partner in Slaughter and May Hong Kong’s Disputes and Investigations department. She joined Slaughter and May’s dispute resolution department in Hong Kong in 2018, focusing on regulatory investigations and inquiries, commercial litigation, and securities investigations. Prior to joining Slaughter and May, Wynne was a Director of Enforcement of the Securities and Futures Commission (SFC), where her principal responsibilities included managing litigation involving the Enforcement Division, giving advice on operational issues encountered by the SFC’s Enforcement Division, and participating in the management of the division.

Rin Moriguchi
*Momo-o, Matsuo & Namba*

Rin Moriguchi is a partner at Momo-o, Matsuo & Namba. Mr Moriguchi has extensive experience in the area of competition law and securities law in addition to corporate, M&A and complex commercial litigation. His broad experience in antitrust and competition law includes more than 10 years of practice since the JFTC initially introduced a leniency programme for corporations’ anti-competitive misconduct. Mr Moriguchi regularly conducts and assists clients’ internal investigations for the purpose of application to leniency programmes and correspondence with competition authorities in multiple jurisdictions. From 2009 to 2010, he served as a specialist officer in the Financial Markets Division of the
Financial Services Agency (FSA). This experience with the FSA led to specialised expertise on issues relating to the financial industry and stock exchanges, governmental investigations, sophisticated financial transactions and shareholder disputes.

Mr Moriguchi received his LLB from Waseda University, Faculty of Law in 2002 and was admitted to the Japanese Bar in 2004. He obtained his LLM from King’s College London in 2014.

MAR DE PEDRAZA
De Pedraza Abogados

Mar de Pedraza is the managing partner of De Pedraza Abogados, a boutique law firm specialising in criminal law, committed to providing its clients with highly sophisticated criminal law advice. Its specialist legal advisory services cover the traditional pre-litigation and litigation side of criminal law cases, in which it represents clients as the defence or prosecution, and the more novel ‘preventive’ side of corporate defence and compliance, which has become a central part of criminal law advice since December 2010.

Prior to establishing De Pedraza Abogados in 2011, Ms de Pedraza worked extensively as a white-collar crime lawyer at some of the most prestigious Spanish and multinational law firms, such as Garrigues and Baker & McKenzie. She studied at the Complutense University of Madrid (1996) and the University of Bologna (1995) and has been a member of the Madrid Bar Association since 1997.

Ms de Pedraza specialises in white-collar crime (such as corruption, bribery, offences against financial and socio-economic interests, fraud, criminal insolvency, misappropriation, misrepresentation and falsification of documents, corporate offences, offences against the tax and social security authorities, among others), corporate compliance and conducting internal investigations (at national and international level).

Ms de Pedraza has been recognised as an expert by various directories and publications. She was the winner of one of Iberian Lawyer’s 40 under Forty Awards 2013 and has been ranked in Band 1 and 2 by Chambers Europe.

STEPHEN PETERS
BDO LLP

Stephen is a forensic accounting partner at BDO in London. He has some 20 years of diverse experience in investigations and litigation matters and international arbitration. Stephen graduated with honours with a BSc degree in civil engineering. He is a fellow of the Institute of Chartered Accountants in England and Wales and has a postgraduate certificate in fraud risk management from John Moores University, Liverpool.

Much of Stephen’s experience involves cross-border disputes and investigations and he has worked throughout the world. He has been involved in expert-witness assignments in the areas of breach of contract and loss of profits, acquisitions and disposals disputes, minority shareholder and joint-venture disputes, insurance claims, valuations, accounts interpretation, directors’ disqualifications and intellectual property matters.

Stephen leads BDO’s contentious insolvency team in the forensic accounting group and regularly works alongside insolvency practitioners in a number of roles: expert witness; adviser; undertaking investigations to follow cash; and tracing and recovery of assets.
JOÃO DANIEL RASSI
Siqueira Castro Advogados

João Daniel Rassi is the head partner of the Corporate Criminal Law Department at Siqueira Castro Advogados. He holds a specialisation in criminal law from Salamanca University, Spain, has received a master’s degree in criminal law from the University of São Paulo (USP) and has a PhD in both criminal law and criminal procedure law from USP.

Throughout more than 25 years working as criminal lawyer, Mr Rassi has participated as defence counsel in a series of media cases, in areas connected to business activities, such as criminal proceedings involving corruption, money laundering, environmental offences, the tax and fiscal system, the financial and capital markets, intellectual property, antitrust and consumer relations, as well as combating corporate and compliance fraud. His professional experience includes negotiations of successfully concluded collaboration agreements with the Office of the Prosecutor General of Brazil.

Mr Rassi has been listed by Chambers and Partners, Latin Lawyer and Análise Advocacia as one of the most respected lawyers in Brazil and Latin America in the area of criminal law and dispute resolution regarding white-collar crimes.

SOURABH RATH
Shardul Amarchand Mangaldas & Co

Sourabh Rath is a senior associate with the firm’s dispute resolution and white-collar defence practice. Sourabh has experience in both internal investigations and criminal investigations and prosecution by federal anti-corruption and anti-money laundering agencies. He has advised and represented Indian and multinational corporations in sensitive anti-corruption and anti-money laundering investigations. His work involves assisting clients and senior management in all aspects of the investigation, advising on defence strategy and representation before courts or in investigations before regulatory and government bodies. Sourabh also has experience in assisting clients with the prosecution of fraud and other economic offences.

KAREN REYNOLDS
Matheson

Karen Reynolds is a partner in Matheson’s commercial litigation and dispute resolution department and is co-head of the regulatory and investigations team. She is regularly instructed in relation to complex contentious regulatory matters and investigations. Karen has particular expertise in financial services disputes, fraud, corporate crime and complex commercial disputes. She advises clients, both corporates and individuals, domestic and international, on a wide range of issues ranging from risk management, reputational issues, bribery, corruption, financial crime and anti-money laundering to enforcement and compliance matters.

FIKRET SEBİLÇIOĞLU
Cerebra CPAs & Advisors

Fikret Sebilcioğlu is the managing partner of Cerebra, an independent accounting and advisory firm based in Istanbul. He has more than 25 years’ experience in the areas of process re-engineering, internal controls, internal audit, forensic accounting, fraud investigation,
anti-bribery, and ethics and compliance initiatives. Prior to Cerebra, Fikret worked with PwC for 15 years from 1993 to 2008 both in Istanbul, Turkey and Rotterdam, The Netherlands. He is a certified fraud examiner (CFE), certified public accountant, registered independent auditor and TRACE anti-bribery specialist. Fikret is a board member of the Ethics and Reputation Society, a board member and vice president of the Transparency International Turkey, a past board member of the Corporate Governance Association of Turkey. He is a lecturer at Ozyegin University, where he delivers business ethics and corporate social responsibility courses to executive MBA students.

DAREN SHIAU
Allen & Gledhill LLP

Daren Shiau, PBM, is a leading regional competition law specialist whose practice covers antitrust litigation, international cartels and merger control. He is Co-Head of the Firm’s Corporate & Commercial Department, and its Competition & Antitrust Practice.

A pioneering competition law specialist in Singapore and ASEAN with unparalleled antitrust experience in Southeast Asia, Daren has been cited as ‘the most highly nominated practitioner’, ‘Singapore’s top competition lawyer’, ‘a real expert according to rivals’, and one of the ‘finest lawyers in the region’ by Who’s Who Legal.

He has successfully advised on more than 70 per cent of Singapore’s merger control cases, acted for the successful amnesty applicant of Singapore’s first global cartel decision, the successful leniency applicant to its second one, and defended parties in 100 per cent of Singapore’s international cartel decisions to date.

Daren has also worked on multiple landmark abuse of dominance cases to date, including the first appeal to the Competition Appeal Board.

A commissioned trainer of the high-level ASEAN Experts Group on Competition, Daren is a Principal Examiner on competition law for the Singapore Institute of Legal Education’s Foreign Practitioners Examinations, and the Singapore Bar Examinations. He is also Singapore’s first appointed non-governmental adviser at the International Competition Network.

KUNAL SINGH
Shardul Amarchand Mangaldas & Co

Kunal Singh is an associate with the firm’s litigation group. He has during the tenure with the firm appeared before various courts in India, in cases related to white-collar crimes such as fraud, breach of trust, cheating and other economic offences. His work also involves assisting the white-collar team in advising clients on investigations under the Foreign Exchange Management Act, 1999 and the Prevention of Money Laundering Act, 2002. He has also advised and represented clients in civil and commercial matters before different courts in India.
HARRIET SLATER
Latham & Watkins

Harriet Slater is an associate in the London office of Latham & Watkins and a member of the litigation and trial department. Ms Slater focuses her practice on white-collar defence, including cross-border criminal government investigations, internal investigations and regulatory investigations.

Ms Slater also has experience in complex commercial litigation across a variety of industries and subject matters, and transaction due diligence including contractual analysis on compliance, corruption, supply chain, sanctions and bribery issues for international clients.

Ms Slater has experience representing clients in the healthcare and banking industries in connection with complex investigations relating to matters before the US and UK governments as well as experience defending individuals in prosecutions by the Serious Fraud Office.

Ms Slater has an active pro bono practice focused on representing individuals in the criminal justice system, as well as supporting rule of law and criminal investigation projects in Sub-Saharan Africa.

JOÃO MATOS VIANA
Morais Leitão, Galvão Teles, Soares da Silva & Associados

João Matos Viana joined the firm in 2001 and became a non-equity partner in 2019. He is head of a criminal and compliance team. He currently practices in the area of litigation, focusing specifically on criminal and administrative offences involving banking, securities, insurance competition and pharmaceutical law. João collaborates regularly in administrative, tax and corporate areas regarding the criminal and administrative matters. João Matos Viana is the author of several articles regarding criminal law and criminal procedure law.

KEVIN WARBURTON
Slaughter and May

Kevin Warburton is a counsel in Slaughter and May Hong Kong’s Disputes and Investigations department. He joined Slaughter and May’s London office in 2007 and, after spending time in the Hong Kong office in 2009 and 2014, relocated there permanently in 2016. He advises a broad range of clients both inside and outside Hong Kong on matters of litigation, arbitration, regulatory investigations and inquiries, data privacy and alternative dispute resolution mechanisms.

LEE BIKEI WEI
Allen & Gledhill LLP

Bik Wei is the Deputy Head of the Firm’s White Collar & Investigations Practice. She regularly advises clients on white-collar, regulatory and compliance and corporate governance matters, and regulatory and corporate investigations. These include matters involving criminal breach of trust, corruption, market misconduct, mutual legal assistance matters, and employee misconduct, fraud, and corporate governance-related issues.
Her main areas of practice also encompass commercial litigation and international arbitration. She has substantial experience in a range of areas including cross-border joint venture disputes, corporate disputes such as shareholder or directors’ disputes, property and trust, and contentious employment disputes.

Bik Wei’s clients include local companies and multinational corporations, both private and listed, and trust companies. Bik Wei is also proficient in Mandarin and has advised Chinese clients in arbitral proceedings.

NORBERT WESS

*wkk law Rechtsanwälte*

Norbert Wess is a founder and partner at wkk law Rechtsanwälte. He graduated from the University of Vienna as Dr iuris and was admitted to the Bar in 2004. Within a short time, he established himself by acting in many of Austria’s high-profile cases concerning white-collar crime. He advises and represents national and international clients (corporations as well as individuals) regarding investigations by Austrian and foreign authorities, and regularly appears in court as a defence counsel, as well as a civil party representative, to enforce their claims as victims of crimes.

Furthermore, Norbert is the author of various publications regarding criminal procedural law and gives lectures and presentations on issues relating to criminal law, compliance and related topics. He is co-editor of the *Journal for Business and Tax Criminal Law* (*Zeitschrift für Wirtschafts- und Finanzstrafrecht*), of the *Manual of Criminal Defense* (*Handbuch Strafverteidigung, 2017*) and of the *Commentary Business Criminal Law* (*Praktikerkommentar Wirtschaftsstrafrecht, 2018*).

Norbert Wess is a member of the board of the Association of Austrian Defence Lawyers (VÖStV), a member of the Commercial Criminal Law Association (WiSteV) and the International Association of Penal Law (AIDP), a member of the disciplinary board of the Vienna Bar Association, and a member and deputy chairman of the disciplinary committee of the Austrian Federal Football League.

ALINE WEY SPEIRS

*Altenburger Ltd legal + tax*

Aline Wey Speirs is a partner at Altenburger Ltd legal + tax. Her practice focuses on litigation, international commercial arbitration and enforcement law. She advises and represents private and corporate clients at all stages of the dispute resolution process.

Aline Wey Speirs has particular expertise in white-collar crime-related matters and in the securing and tracing of assets. She has represented clients in multi-jurisdictional trust litigations, commercial disputes, bankruptcy and debt collection procedures. In addition, she has broad experience in enforcing judgments and arbitral awards.

MAIR WILLIAMS

*Latham & Watkins*

Mair Williams’ practice focuses on white collar defence. She has considerable trial experience, having started her career as a criminal barrister in chambers, as well as experience in investigations, representing companies and individuals before regulators and prosecuting bodies, and developing compliance policies and practices for international clients.
In addition to her white-collar work, Ms Williams has experience in all manner of complex commercial litigation and has represented clients at every stage from initial pleadings through to trial and appeal. She has worked with clients from all manner of industries including financial services, media, food and beverage, manufacturing and technology.

Ms Williams has conducted a range of internal investigations in jurisdictions across the world including an investigation of a financial services firm following a leak of confidential information to the media, and an investigation on behalf of a private pension scheme following allegations made by a whistle-blower. Her diverse range of representative experience includes representing a director in an investigation by the Financial Reporting Council into discrepancies with annual accounts of a FTSE 250 company and representing a publicly listed investment firm in investigations by the Financial Conduct Authority and Serious Fraud Office.

Ms Williams is a passionate pro bono advocate and her practice is focused on representing individuals in the criminal justice system, particularly post-conviction.

MARIO ZANCHETTI

Studio Legale Pulitanò-Zanchetti

Mario Zanchetti is a founding partner of Studio Legale Pulitanò-Zanchetti, which has its main office in Milan. He practises extensively in business criminal law, criminal liability of corporations, banking and money laundering law and regulations, environmental crimes and criminal liability for industrial accidents.

For the past 25 years, Professor Zanchetti has represented the top managers of Italian and multinational corporations, and the corporations themselves, in several high-profile cases.

He graduated magna cum laude from the Catholic University of Milan in 1984 and was admitted to the Italian Bar in 1988. In 2001, he qualified to appear before the Supreme Court.

Between 1998 and 2000, he served as associate professor of criminal law at University of Bari. Since 2000, he has been a full professor of criminal law at University Carlo Cattaneo in Castellanza. Professor Zanchetti was Dean of the Faculty of Law of University Carlo Cattaneo from 2000 to 2012.

He has been a member of the scientific committee of the pharmacology master’s degree at the University of Milan since 2003 and is president of the criminology master’s degree course at the University Carlo Cattaneo. Professor Zanchetti is the author of more than 60 publications on criminal law.

JERINA (GERASIMOULA) ZAPANTI

Anagnostopoulos

Jerina (Gerasimoula) Zapanti is a member of the Athens Bar (2001) and the Hellenic Criminal Bar Association (2007). She has multi-year experience in cases of corporate compliance, money laundering and cross-border criminal proceedings. She is frequently involved in internal corporate investigations and risk management assessment for national and multinational corporations.
ALAN ZHOU

Global Law Office

Alan Zhou is a partner at Global Law Office based in Shanghai. His practice is focused in the areas of general corporate, transactions, compliance and risk control. As an expert on legal issues surrounding mergers and acquisitions, compliance and tax of foreign investment in China, Mr Zhou has extensive experience in solving complex and challenging issues, advice on creative and strategic solutions.

Mr Zhou has a particularly strong background in the life and health industry. He has routinely represented multinational corporations. As a participant or as an external counsel, Mr Zhou has been engaged by local authorities and industrial associations for advising on legislation and industrial standards in the life and health industry, topics of which including online hospital, digital marketing, medial insurance reform, medical representative management, and other compliance topics.

Mr Zhou has worked with Boehringer Ingelheim China as the general counsel in China for over nine years and is responsible for various legal matters including general corporate, acquisitions and joint venture formation, regulatory compliance, intellectual property and corporate restructure. Mr Zhou has been ranked as a leading practitioner in healthcare and M&A by Chambers and Partners 2012–2019 and selected as a leading practitioner in mergers and acquisitions in the Legal Media Group’s Expert Guides.
CONTRIBUTORS’ CONTACT DETAILS

ALLEN & GLEDHILL LLP
One Marina Boulevard, 28-00
Singapore 018989
Tel: +65 6890 7188
Fax: +65 6327 3800
jason.chan@allenandgledhill.com
lee.bikwei@allenandgledhill.com
vincent.leow@allenandgledhill.com
daren.shiau@allenandgledhill.com
www.allenandgledhill.com

BDO LLP
55 Baker Street
London
W1U 7EU
United Kingdom
Tel: +44 20 7486 5888 / +44 20 893 3480
Fax: +44 20 7487 3686 / +44 20 7487 3686
stephen.peters@bdo.co.uk
nat.butcher@bdo.co.uk
www.bdo.co.uk

ALTENBURGER LTD LEGAL + TAX
Seestrasse 39
8700 Kusnacht-Zurich
Switzerland
Tel. +41 58 810 22 22
Fax +41 58 810 22 25
wey@altenburger.ch
www.altenburger.ch

BRUCHOU, FERNÁNDEZ MADERO & LOMBARDI
Ing. Enrique Butty 275, 12th Floor
C1001AFA, Buenos Aires
Argentina
Tel: +54 11 4021 2345 / 5171 2345
Fax: +54 11 4021 2301 / 5171 2301
fernando.basch@bruchou.com
guillermo.jorge@bruchou.com
gabriel.lozano@bruchou.com
www.bruchou.com

ANAGNOSTOPOULOS
Odos Patriarchou Ioakeim 6
106 74 Athens
Greece
Tel: +30 210 729 2010
Fax: +30 210 729 2015
ianagnostopoulos@iag.gr
jzapanti@iag.gr
www.iag.gr
Contributors’ Contact Details

CEREBRA CPAS & ADVISORS
Büyükdere Cad. No. 103/A
Şarlı İş Merkezi K. 5 34394
Mecidiyeköy-Şişli
İstanbul
Turkey
Tel: +90 212 291 91 76
Fax: +90 212 291 90 04
fikretsebilcioglu@cerebra.com.tr
www.cerebra.com.tr

GLOBAL LAW OFFICE
35th & 36th Floor, One ICC, Shanghai ICC
999 Middle Huai Hai Road, Xuhui District
Shanghai 200031
China
Tel: +86 21 2310 8200 / 8211
Fax: +86 21 2310 8299
alanzhou@glo.com.cn
jackyl@ glo.com.cn
www.glo.com.cn/en

CMS VON ERLACH PONCET LTD
Dreikönigstrasse 7
8022 Zurich
Switzerland
Tel. +41 44 285 11 11
Fax +41 44 285 11 22
bernhard.loetscher@cms-vep.com
cms.law

KOLCUOĞLU DEMİRKAN
KOÇAKLI
Sağlam Fikir Sok. Kelebek Çıkmazı No. 5
Esentepe, Şişli
İstanbul
Turkey
Tel: +90 212 355 99 00
Fax: +90 212 355 99 99
odemirkan@kolcuoglu.av.tr
bbicer@kolcuoglu.av.tr
www.kolcuoglu.av.tr

DEBEVOISE & PLIMPTON LLP
4 place de l’Opéra
75002 Paris
France
Tel: +33 1 40 73 12 12
Fax: +33 1 47 20 50 82
abisch@debevoise.com
ftdavis@debevoise.com
tjenkins@debevoise.com
akirry@debevoise.com
www.debevoise.com

LATHAM & WATKINS
99 Bishopsgate
London EC2M 3XF
United Kingdom
Tel: +44 20 7710 1000
Fax: +44 20 7374 4460
stuart.alford.qc@lw.com
mair.williams@lw.com
harriet.slater@lw.com
www.lw.com

DEPEDRAZA ABOGADOS SLP
Calle de Antonio Maura 10
3rd Floor
28014 Madrid
Spain
Tel: +34 91 532 39 43
Fax: +34 91 523 98 70
mar@depedraza.com
paula.mbarros@depedraza.com
www.depedraza.com

LINKLATERS LLP
Rue Brederode 13
1000 Brussels
Belgium
Tel: +32 2 501 95 21
Fax: +32 2 501 94 94
stefaan.loosveld@linklaters.com
sarah.benzidi@linklaters.com
www.linklaters.com
MATHESON
70 Sir John Rogerson’s Quay
Dublin 2
Ireland
Tel: +353 1 232 2000
Fax: +353 1 232 3333
ciara.dunny@matheson.com
karen.reynolds@matheson.com
www.matheson.com

SETTERWALLS ADVOKATBYRÅ AB
Sturegatan 10
114 36 Stockholm
Sweden
Tel: +46 8 598 890 00
Fax: +46 8 598 890 90
ulf.djurberg@setterwalls.se
ronja.kleiser@setterwalls.se
www.setterwalls.se

MOMO-O, MATSUO & NAMBA
Kojimachi Diamond Building
4-1 Kojimachi, Chiyoda-Ku
Tokyo 102-0083
Japan
Tel: +81 3 3288 2080
Fax: +81 3 3288 2081
moriguchi@mmn-law.gr.jp
ryota.asakura@mmn-law.gr.jp
www.mmn-law.gr.jp

SHARDUL AMARCHAND MANGALDAS & CO
Amarchand Tower
216, Okhla Industrial Estate Phase 3
New Delhi 110020
Delhi
India
Tel: +91 11 4159 0700
anuj.berry@amsshardul.com
nishant.joshi@amsshardul.com
sourabh.rath@amsshardul.com
kunal.singh@amsshardul.com
www.amsshardul.com

MORAIS LEITÃO, GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS
Rua Castilho, 165
Lisbon 1070-050
Portugal
Tel: +351 21 381 74 00
Fax: +351 21 381 74 99
jmvianna@mlgts.pt
jlcluny@mlgts.pt
tcmagalhaes@mlgts.pt
www.mlgts.pt

SHIN & KIM
23th Floor, D-Tower (D2)
17 Jongno 3-gil, Jongno-gu
Seoul 03155
South Korea
Tel: +82 2 316 4114
Fax: +82 2 756 6226
sjinchoi@shinkim.com
tkhong@shinkim.com
kjchoi@shinkim.com
www.shinkim.com

NYMAN GIBSON MIRALIS
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia
Tel: +61 2 9264 8884
Fax: +61 2 9264 9797
dm@ngm.com.au
pg@ngm.com.au
jc@ngm.com.au
www.ngm.com.au

© 2020 Law Business Research Ltd
SIQUEIRA CASTRO ADVOGADOS
Rua Tabapuã, No. 81, 4th Floor
Itaim Bibi
São Paulo 04533-010
Brazil
Tel: +55 11 3704 9840
Fax: +55 11 3704 9848
rassi@siqueiracastro.com.br
vlabate@siqueiracastro.com.br
placamargo@siqueiracastro.com.br
www.siqueiracastro.com.br

SLAUGHTER AND MAY
47th Floor, Jardine House
1 Connaught Place Central
Hong Kong
Tel: +852 2521 0551
Fax: +852 2845 2125
wynne.mok@slaughterandmay.com
kevin.warburton@slaughterandmay.com
www.slaughterandmay.com

SŁOTYSIŃSKI Kawecki & Szlęzak
ul. Jasna 26
00-054 Warsaw
Poland
Tel: +48 22 608 70 00
Fax: +48 22 608 70 70
tomasz.konopka@sksemail.pl
www.sksemail.pl

STUDIO LEGALE PULITANÒ-ZANCHETTI
Via Bianca di Savoia No. 9
Milan 20122
Italy
Tel: +39 02 4548 5700
Fax: +39 02 4548 5701
m.zanchetti@studiolegalepz.it
www.studiolegalepz.com

SULLIVAN & CROMWELL LLP
125 Broad Street
New York
NY 10004-2498
United States
Tel: +1 212 558 4000
Fax: +1 212 558 3588
bourtinn@sullcrom.com
hsichst@sullcrom.com
www.sullcrom.com

WKK LAW RECHTSANWÄLTE
Himmelpfortgasse 20/2
1010 Vienna
Austria
Tel: +43 (0) 1 532 13 00
Fax: +43 (0) 1 532 13 90
n.wess@wkk.law
m.machan@wkk.law
v.mcallister@wkk.law
www.wkk.law