THE INTERNATIONAL INVESTIGATIONS REVIEW

EIGHTH EDITION

Editor
Nicolas Bourtin

© 2018 Law Business Research Ltd
ACKNOWLEDGEMENTS

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

ALLEN & GLEDHILL LLP
ALVAREZ & MARSAL DISPUTES AND INVESTIGATIONS, LLP
ANAGNOSTOPOULOS
BDO LLP
BOFILL ESCOBAR ABOGADOS
CMS VON ERLACH PONCET LTD
DEBEVOISE & PLIMPTON LLP
DE PEDRAZA ABOGADOS, SLP
HORTEN LAW FIRM
KHAITAN & CO
LINKLATERS LLP
MATHESON
MOMO-O, MATSUO & NAMBA
NYMAN GIBSON MIRALIS
R&T ASIA (THAILAND) LIMITED
SETTERWALLS ADVOKATBYrå AB
SHIN & KIM
SIQUEIRA CASTRO ADVOGADOS
SLAUGHTER AND MAY
SOŁTYSIŃSKI KAWECKI & SZLĘZAK
STEPTOE & JOHNSON UK LLP
Acknowledgements

STUDIO LEGALE PULITANO-ZANCHETTI
SULLIVAN & CROMWELL LLP
WKK LAW RECHTSANWÄLTE
# CONTENTS

PREFACE .......................................................................................................................................................... vii
Nicolas Bourtin

Chapter 1  THE ROLE OF FORENSIC ACCOUNTANTS IN INTERNATIONAL INVESTIGATIONS................................................................. 1
  Gavin Williamson and Stephen Peters

Chapter 2  DIGITAL FORENSICS .................................................................................................................. 7
  Phil Beckett

Chapter 3  EU OVERVIEW .......................................................................................................................... 19
  Stefaan Loosveld

Chapter 4  AUSTRALIA ................................................................................................................................. 25
  Dennis Miralis and Phillip Gibson

Chapter 5  AUSTRIA .................................................................................................................................. 37
  Norbert Wess, Vanessa McAllister and Markus Machan

Chapter 6  BELGIUM .................................................................................................................................. 48
  Stefaan Loosveld

Chapter 7  BRAZIL ......................................................................................................................................... 60
  João Daniel Rassi, Gauthama C C Fornaciari de Paula and Victor Labate

Chapter 8  CHILE .......................................................................................................................................... 70
  Jorge Bofill and Daniel Praetorius

Chapter 9  DENMARK................................................................................................................................... 83
  Jacob Møller Dirksen
<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>John Rupp, Alex Melia, Peter Ibrahim and Andris Ivanovs</td>
<td>91</td>
</tr>
<tr>
<td>11</td>
<td>FRANCE</td>
<td>Antoine Kirry, Frederick T Davis and Alexandre Bisch</td>
<td>114</td>
</tr>
<tr>
<td>12</td>
<td>GREECE</td>
<td>Ilias G Anagnostopoulos and Jerina (Gerasimoula) Zapanti</td>
<td>128</td>
</tr>
<tr>
<td>13</td>
<td>HONG KONG</td>
<td>Mark Hughes and Kevin Warburton</td>
<td>136</td>
</tr>
<tr>
<td>14</td>
<td>INDIA</td>
<td>Anand Mehta, Susmit Pushkar, Vinay Joy and Supratim Chakraborty</td>
<td>148</td>
</tr>
<tr>
<td>15</td>
<td>IRELAND</td>
<td>Karen Reynolds, Claire McLoughlin and Nicola Dunleavy</td>
<td>160</td>
</tr>
<tr>
<td>16</td>
<td>ITALY</td>
<td>Mario Zanchetti</td>
<td>173</td>
</tr>
<tr>
<td>17</td>
<td>JAPAN</td>
<td>Kakuji Mitani and Ryota Asakura</td>
<td>188</td>
</tr>
<tr>
<td>18</td>
<td>KOREA</td>
<td>Seong-Jin Choi, Tak-Kyun Hong and Alex Kim</td>
<td>199</td>
</tr>
<tr>
<td>19</td>
<td>POLAND</td>
<td>Tomasz Konopka</td>
<td>209</td>
</tr>
<tr>
<td>20</td>
<td>SINGAPORE</td>
<td>Jason Chan, Vincent Leow and Daren Shiau</td>
<td>219</td>
</tr>
<tr>
<td>21</td>
<td>SPAIN</td>
<td>Mar de Pedraza and Paula Martinez-Barros</td>
<td>232</td>
</tr>
<tr>
<td>22</td>
<td>SWEDEN</td>
<td>Ulf Djurberg and Softe Ottuson</td>
<td>244</td>
</tr>
</tbody>
</table>
In the United States, it is 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 several years, 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 new presidential administration in 2017 brought uncertainty about certain enforcement priorities, there have been few signs – even a year and a half into the new administration – of any significant departure from the trend towards more enforcement and harsher penalties.

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 eighth edition, this publication covers 23 jurisdictions.

This volume is the product of exceptional collaboration. I wish to commend and thank our publisher and all the contributors for their extraordinary gift 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
July 2018
Chapter 1

THE ROLE OF FORENSIC ACCOUNTANTS IN INTERNATIONAL INVESTIGATIONS

Gavin Williamson and Stephen Peters

I INTRODUCTION

As the number and scale of international investigations has multiplied during the past few years, forensic accountants have been used by companies and their legal counsel to fulfil a wide range of investigative roles outside purely technical financial analysis. A forensic accounting practice will now typically offer forensic technology and e-disclosure services, large-scale document review capability, corporate intelligence skills and the ability to undertake general investigation, including interviewing witnesses and suspects.

This diversification in the role of the forensic accountant is at least in part 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, and therefore, offers UK-based or US-based organisations and legal counsel the ability to deploy local resources quickly. It also represents recognition on the part of legal counsel that aspects of large international investigations are heavily process-driven and that their skills and experience may be better focused on strategy and litigation.

The involvement of the forensic accountant in international investigations follows a typical arc: investigating the facts and circumstances around the matter 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 supporting recovery efforts. The size and diversity of offerings found in the larger accounting firms also allows an investigation team to, for instance, bring in specific sector specialisms or harness the skills of insolvency practitioners and valuation experts to support recovery efforts. Indeed the modern ‘investigative’ forensic accountant may be defined as much by his or her armoury of tools and techniques that he or she can bring to a matter, as by his or her traditional core set of accountancy skills; understanding the principles of asset tracing in equity or predictive coding in e-disclosure is now as important as an appreciation of the workings of a balance sheet.

II FORENSIC ACCOUNTING

The traditional role of the forensic accountant in investigations has been focused on the analysis of financial and accounting records. Most forms of fraud, bribery and general financial misconduct can be identified in, and evidenced through, the financial and accounting records
of an organisation. While a payment, loss or unauthorised transaction may be disguised or hidden, its existence must often be recognised in the accounts, an absence producing an imbalance or reconciliation error and a ‘red flag’ for management and auditors.

The focus of forensic financial analysis and the extent to which it is required depends on the nature of the subject of the investigation. The direct cost of bribes to an organisation may be recorded in the accounts payable ledger, employee expenses, commissions or accounts receivable ledger as discounts. The direct cost of procurement fraud may be recorded in the accounts payable ledger and aggressive revenue recognition will be reflected in the accounts receivable ledger and sales records. Even where a fraud 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, the technicalities of their underlying transactions and even terminology and jargon vary significantly between industry sectors, geographically, and from the smallest to largest organisations. Having the right mixture of forensic accounting and sector-specific knowledge and experience in the investigation team is essential; it may, for instance, be necessary to include project accounting experience for an engineering firm investigation, or specific Forex or derivative valuation experience for a banking investigation.

### Investigative interviewing

Interviews are a key component of a forensic accountant’s work. The analysis of accounting records without the context and direction provided by witness and suspect interviews may become simply an intellectual exercise and fail to progress an investigation. 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. While the interview process may be led by legal counsel, where a fraud or its concealment involves even moderately complex accounting treatment, it is likely to be beneficial to include forensic accountants in the relevant interviews.

### III ELECTRONIC DOCUMENT REVIEW AND E-DISCLOSURE

Computers, phones and other mobile devices are features of our modern existence and nowadays a large proportion of our personal and corporate records exist in electronic format. The volume of records that we hold has exploded: a single computer can hold several million documents; a typical electronic mailbox may hold anything from 50 to 100,000 emails. The volume of potentially relevant records of a large company involved in an international investigation may therefore number in the hundreds of millions. Technology is also revolutionising the mechanisms by which people communicate with each other, even within traditional organisations. It is increasingly our ability to collect and review such diverse communications as instant messaging, Skype, text messaging and mobile phone applications such as WhatsApp and Facebook Messenger, that is the key to identifying wrongdoing and those colluding in it.

In a post-Snowden environment, encryption is becoming more widely adopted by both the business world and the public alike. Advances in encryption technology, however, are often matched by advances in forensic technology. As a recent example, the developers of WhatsApp, an instant messaging mobile phone application, publicly announced end-to-end encryption for all communications. Within a single month, the leading provider of mobile phone forensic software had developed a solution to decrypt WhatsApp data and rolled out...
the software fix to all its licence holders. As a result, the use of encryption has not yet become sufficiently widespread or effective to significantly limit the volume of potentially relevant data becoming available for review.

Conventional document-review methodologies allow hundreds of millions of documents to be automatically filtered down to mere tens of thousands for manual review with the application of suitable search terms. With a reliable internet connection, reviewers can be sourced from and based anywhere in the world, allowing legal teams, forensic accountants and specialist language reviewers to combine across jurisdictions. This process of electronic document review and disclosure is now well established and such is its ease, effectiveness and speed of use that physical documents are generally best scanned and reviewed electronically. Manual review of large numbers of documents remains costly, however, and as data volumes and disclosure exercises in international investigations continue to grow, simple keyword filtering may be beginning to reach the end of its usefulness. This has encouraged increased adoption of two connected forms of advanced technology: concept searching and predictive coding.

i Concept searching

Even the simplest modern e-disclosure software now has the functionality to perform concept searches based on powerful statistical algorithms. A concept search identifies all documents containing the search term and goes further, identifying additional documents relevant to the idea of the search term; thus, searching for ‘Christmas’ may also identify documents relating to gift ideas or turkey recipes, and searching for ‘football’ may also identify documents relating to different teams, stadiums or sponsors. In this way concept searching enables a more complete and intelligent enquiry, allowing the reviewer to get quickly to a fuller set of relevant information and, used carefully, can minimise the number of false positives presented for manual review.

ii Predictive coding

Predictive coding, which was approved in 2016 for use in an English court for the first time in Pyrrho Investments v. MWB Property,² offers even greater opportunities for improvement in efficiency and cost savings. Sometimes called ‘technology-assisted review’, predictive coding relies on e-disclosure software to identify relevant documents based on a limited but representative ‘seed set’ of manually reviewed documents. The software identifies concepts within documents manually identified as relevant within the seed set to return all similar documents from the overall data population. A further limited set of documents returned is then selected and another manual review performed, and the software uses the results of the quality review to refine its understanding of relevance. With each iteration, the computer learns to distinguish what is relevant, and each iteration produces an increasing small set of ever more relevant documents. Most importantly it significantly reduces the number of irrelevant documents subject to manual review and thus the overall cost of document review and disclosure process. As Master Matthews states in Pyrrho Investments v. MWB Property: “This technology saves time and reduces cost. Moreover, unlike with human review, the cost does not increase at the same rate as the number of documents to review increases. So doubling the number of documents does not double the cost.”

² [2016] EWHC 256 (Ch).
The use of predictive coding is more advanced in the United States and there, again, cost has been the major factor in its use. In addition, there is growing evidence that, when properly conducted, the failure rate of predictive coding can actually be lower than that of a manual review team. There is every indication, therefore, that electronic document review and thus large-scale international investigation is becoming more effective, less expensive and significantly faster.

IV ASSET TRACING

The nature of international investigations is such that we are commonly dealing with financially astute fraudsters who are able to take significant steps to move and hide their stolen proceeds, and frustrate recovery attempts by legitimate owners. Assets are transferred between accounts, moved outside the jurisdiction in which they were stolen, divided up and dissipated, and placed within and behind various corporate devices and trusts as a means of disguising the link between the fraudster, the stolen assets and those seeking legitimate recovery. Because of its fungibility and speed of movement, tracing cash is difficult, and while real property can be easier to locate, its ownership can be disguised through the use of offshore companies, trusts and Anstalten and other corporate devices.

Victims of this type of crime 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 include a more or less iterative process of gathering and analysing evidence of asset movement, securing and freezing identified assets, and applying legal remedies such as search and third-party disclosure orders to obtain further evidence of asset movement. A division of labour between legal counsel and the forensic accountant very quickly establishes itself, with the latter focusing on the messy and complex business of analysing financial, corporate and banking records to ‘follow the money’.

Banking records in particular are the bread and butter of a forensic tracing exercise, representing an accurate and reliable source of evidence. Indeed, frequently the only record of a flow of assets will be held by the financial institution facilitating the transaction.

It is important to note that asset tracing, while governed by the ‘rules’ of both common law and, to a greater extent, equity, is not a legal end in itself. Lord Millet described it as ‘neither a claim nor a remedy. It is merely a process by which a claimant demonstrates what has happened to his property, identifies its proceeds and the persons who have handled or received them, and justifies his claim that the proceeds can properly be regarded as representing his property’.3

Traditionally, tracing has been 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. It has also been restricted by the ‘lowest intermediate balance’ principle, whereby a claimant’s ability to trace funds into a bank account is limited to the lowest balance held between the date of misappropriation and the date on which the claim is brought, even if funds were subsequently paid into the bank account so as to restore the balance.


© 2018 Law Business Research Ltd
A simple application of these tracing rules is susceptible to being defeated by a sophisticated money launderer. For instance, if a loan has been taken out to pay for a property and misappropriated funds are used later to pay off the loan, the beneficiary’s property could be said to have been dissipated (i.e., used to discharge a liability). However, in two recent cases, English courts have demonstrated significant flexibility in the application of these tracing rules.

i ‘Backwards’ tracing

In *Relfo Ltd (in liquidation) v. Varsani,* the court accepted the principle that if a payment is made by one intermediate party in advance of receiving reimbursement from traceable funds, that is sufficient to trace a flow of funds or substitute property to its ultimate destination. This is often described as ‘backwards tracing’ and in certain circumstances allows a claimant’s property to be traced to an asset already in the possession of the defendant.

In *Federal Republic of Brazil v. Durant International Corporation (Jersey),* the Privy Council also accepted the use of backwards tracing where past payments could be demonstrated to be linked to the expectation of reimbursement from traceable funds:

> The development of increasingly sophisticated and elaborate methods of money laundering, often involving a web of credits and debits between intermediaries, makes it particularly important that a court should not allow a camouflage of interconnected transactions to obscure its vision of their true overall purpose and effect. . . . If the court is satisfied that the various steps are part of a coordinated scheme, it should not matter that, either as a deliberate part of the choreography or possibly because of the incidents of the banking system, a debit appears in the bank account of an intermediary before a reciprocal credit entry.

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, although 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, and so on.

---

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 United Kingdom are accountants or insolvency experts working in firms of chartered 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, is likely to 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 be likely to involve the skills and expertise of a forensic accountant, this time not in a purely investigative capacity but as an adviser on quantum. The forensic accountant would assist 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 Rules Part 35, or its equivalent in overseas jurisdictions, should the matter proceed to litigation.
I  INTRODUCTION

This chapter looks at the importance of forensic technology within investigations. It starts by looking at why data is so crucial to an investigation, before examining the different types of data available to an investigator. It then discusses the processes that should be followed to capture, prepare and investigate data to ensure that it is incorporated into an investigation appropriately before discussing how artificial intelligence and machine learning can assist the investigator.

II  CRITICALITY OF DATA TO AN INVESTIGATION

Data is the lifeblood of most modern-day organisations: this is no less true for an investigator. Although not the only source of information relevant to an investigation, data can provide an unbiased, unaltered and accurate reflection of historic events unlike other sources. Data can be more reliable than the human mind, especially if the relevant events are historic, and data tends to be more pervasive and persistent than paper documents. Forensic technology is the practice of dealing with data in such a way that it can be incorporated into an investigation in a legally admissible form.

When conducting an investigation, it is essential that data is fully incorporated within the overall scope of the investigation. Not only does data need to be included, it should be central to the investigative process and not viewed as a separate, stand-alone task. As with other aspects of an investigation, the process is more efficient and effective if the different aspects are connected and the findings flow between them in a timely manner. The key goal is to empower the investigation through the intelligent analysis and investigation of data.

However, data tends to be highly volatile and can easily be altered or deleted, intentionally or otherwise; therefore it is important that the process of managing data in an investigative sense is dealt with at an early stage of the investigation, in a forensically sound matter and in an all-encompassing way. This does not mean that every single byte of data needs to be fully investigated, just that all relevant systems need to be appropriately considered.

---

1 Phil Beckett is managing director at Alvarez & Marsal Disputes and Investigations, LLP.
When it comes to managing data in a forensically sound manner, the Association of Chief Police Officers’ (ACPO) Good Practice Guide for Digital Evidence\(^2\) provides a sound basis for any investigator, specifically the four principles it promotes:

*Principle 1:* No action taken . . . should change data which may subsequently be relied upon in court.

*Principle 2:* In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

*Principle 3:* An audit trail or other record of all processes applied to digital evidence should be created and preserved. . .

*Principle 4:* The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

It is essential during an investigation that the process followed to capture, prepare and investigate data is robust and complete, otherwise the results may not be admissible in a court of law or the investigation itself may become publicly criticised.

### III TYPES OF DATA AVAILABLE TO AN INVESTIGATOR

Given the use of technology throughout a workplace and beyond, data exists in many different forms and sources, but can be considered within a two-dimensional grid, as illustrated below:

<table>
<thead>
<tr>
<th>Table 1: Framework for understanding data types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of data</strong></td>
</tr>
<tr>
<td>Unstructured</td>
</tr>
<tr>
<td>Structured</td>
</tr>
<tr>
<td>Social</td>
</tr>
</tbody>
</table>

All these sources need to be considered in regard to an investigation; however, for the purposes of this chapter, I will not differentiate between internal and external sources, as from a technical perspective the approach is the same – although the practical and legal considerations vary greatly.

Unstructured data refers to information that does not have a pre-defined structure and is typically text-heavy, but may contain dates, numbers, graphics and other types of information. It is the form of data that we are probably most familiar with and would include emails, documents, spreadsheets and presentations. Typical sources of unstructured data would include:

- a computers, be it a laptop, desktop or workstation;
- b mobile phones and tablets, which tend to be more and more central to an investigation;
- c email systems, including archives;
- d network file shares, including but not limited to personal ‘home’ drives, departmental drives and profiles within a typical organisation; and
- e other document repositories within an organisation, for example SharePoint servers.

Although the above sources will contain a myriad of different file types, including music, videos and system files, unless there are specific reasons why they should be included in an investigation, typically, the investigation will focus on user-generated files such as emails, documents, spreadsheets and presentations, with the rest being filtered out.

Structured data is the opposite of unstructured data, in that it refers to information that does have a pre-defined structure and is generally in the form of ‘databases’, but can be much wider than this. In respect of an investigation, the most common sources of structured data relate to systems that monitor or record activity related to the substance of the investigation; for example, accounting and banking records in respect of a financial fraud, or expense claims in respect of an expense fraud.

A hybrid of structured and unstructured data, referred to as semi-structured data, can also be prevalent within an organisation: this is where the content tends to be unstructured but it is bound by a more solid structure. A typical example of this would be chat or instant messenger messages, which can be very revealing to an investigation and therefore should not be overlooked.

Social data is a relatively new class referring to data that is shared publicly, or in a more restricted context (e.g., within an organisation or a circle of ‘friends’), which is stored within a central repository and includes not only the content but also information that is linked to this content, such as shares, likes, location, time posted, and so on. Although the most recognisable sources will be external to an organisation (e.g., Facebook, LinkedIn), many organisations are using these technologies internally and thus they need to be included within an investigation.

When considering these different sources of data, it is important that they are not simply considered from a technical perspective, as it is easy to get swamped by data when collecting everything due to the sheer volume created and captured by modern companies. Other factors can influence what and how different sources are dealt with during an investigation, for example:

- **Time:** it is important to consider which sources of data were actually in use at the time the investigation relates to, as opposed to the ones in operation currently.
- **Backups:** all organisations should have some sort of backup policy implemented across some or all of their systems. It is important that the above-mentioned sources are considered as they can provide a timely snapshot of activity from a historical moment in time. This can be particularly useful if there are any suspicions of data being deleted.
- **Custodian scope:** it is essential to also consider the human element during an investigation, ensuring that the right people are considered in the scope of the investigation; this will also drive the sources to be considered, as not all people have access to all sources. Two important points here are:
  - to recognise that not all processes (see later) need to be applied to all custodians or data sources. Therefore, it is generally more appropriate to cast a wider net at the start of the investigation but then focus on key custodians or data sources; and
  - that ‘witnesses’ as well as ‘suspects’ should be included in the process. Typically this will include assistants as they often store much more data than the people they work for.
- **Actual usage:** there is often a wide variance within an organisation between how IT think computer systems are used within their organisation and how individuals actually use them. For an investigation, it is the latter that is important.
It is also critical when considering all the above data types that hard-copy or paper sources are not forgotten or overlooked, although they should be fully integrated into the investigation process, as discussed later.

IV PROCESSES TO FOLLOW TO MAXIMISE THE USE OF DATA IN AN INVESTIGATION

When dealing with data in respect of an investigation, the exact way that it is managed and implemented will vary from case to case; however, there are various models available that set out some of the key stages of such exercises. The most widely used, and referenced, is the ‘Electronic Discovery Reference Model’, which was designed to meet the requirements of legal discovery under US litigation and it has equal applicability to how you can manage data during an investigation. A more simplified model for investigations that I have used comprises five key stages:

a identification;
b collection;
c processing;
d data repository; and
e investigation and analysis.

The first stage is designed to identify the entire universe of systems that may hold relevant documents, which can be very varied (as described above). A data-mapping exercise is a core component of this, and is most effectively compiled by having timely discussions about the systems in place at the relevant time with both members of the IT team and individual users. With this dual perspective, as described above, it is possible to establish and document which systems could hold relevant documents, not only from a theoretical perspective (i.e., how systems should have been used) but also from a practical perspective (i.e., how systems were actually used). Once collated, the identified systems can be analysed to determine their potential relevance to the investigation.

One key difference when dealing with an investigation, as opposed to a discovery or disclosure exercise, is that the concept of proportionality does not apply to the same degree – especially in the context of regulatory driven investigations, whereby the actions performed within an investigation can be scrutinised as thoroughly as the findings. This generally means applying a wider scope to the exercise when determining the relevance of systems and individuals to an investigation, and thereby deciding whether to collect data related to them.

The collection phase of an investigation consists of two separate components: preservation and the actual forensic collection. The key goal with preservation is to ensure that nothing relevant to the investigation is ‘lost’ or compromised. Typically this will involve taking steps, such as those listed below, to ensure that relevant data should be available as and when needed during the investigation:

a activating litigation hold procedures and mechanisms;
b prohibiting backups from being recycled or deleted;
c ensuring all automatic archiving or deletion processes are suspended;

---

suspensing the wiping and reissuing of any physical devices (e.g., computers and smartphones); and

enabling journaling (or equivalent) on any email or chat system.

The second phase is the actual forensic collection of data, complying with the ACPO guidelines for digital evidence, as discussed above, which have become the standard to which all forensic practitioners should comply to ensure that collection exercises cannot be challenged. It is important to note here that to preserve some forms of data, a forensic image is the most practical solution – especially when dealing with physical devices such as computers and smartphones. However, whereas the scope of the preservation should be set in the widest possible context, the scope of any forensic collection exercises would tend to be more targeted, although still broad enough for the purposes of the investigation.

Once the relevant data has been securely collected and backed up, then the data needs to be processed into a single data repository, so that the contents can be thoroughly analysed, investigated and reviewed. This stage has effectively three phases:

a. identifying which documents (or data) from the collected systems are to be processed. This does not necessarily mean the entire universe of collected data;

b. the documents or data selected then, in certain cases, need to be converted or normalised to ensure that they can be handled effectively in latter stages of the process; and

c. the documents and data then need to be loaded into a single data repository. This typically also includes performing:

• compound file expansion, to ensure that the individual files, records and emails from containers (e.g., ZIP, RAR, PST files) are included as separate records within the data repository, otherwise they can be overlooked;

• signature analysis, to identify the true file type of each file, rather than relying on the simple file extension, which can be altered by the user, to ensure that files are categorised and analysed correctly;

• deduplication, to ensure that only single instances of each document exist in the repository, although it is important to be able to track where any duplicates existed, as sometimes seeing who had access to which documents, and when, can be very important;

• near deduplication, which is an extension of deduplication but focuses on the actual content within a document (as opposed to its form and metadata) and provides a degree of similarity (e.g., 95 per cent identical in content) to determine whether two documents are considered near duplicates;

• email threading, so that chains of emails can be identified and grouped together to enable the investigator to look at the complete sequence of communication in one place, as opposed to seeing the different components piecemeal and multiple times;

• indexing, so that documents can be searched;

• latent semantic indexing (or similar), so that the key concepts and phrases can be identified and searched during an investigation, rather than just the individual words;

• language identification, so that documents containing foreign languages can be identified and directed towards appropriately fluent investigators; and

• optical character recognition across relevant ‘images’ so that any text they contain can also be made searchable.
The ideal end result is that all selected data is processed in its entirety and can be made available to the investigators through a single repository. The concept of a single repository is crucial to a successful investigation as it enables all data and documents, irrespective of form or source, to be analysed through a single lens. This enables intelligence from different documents and sources to be considered together, in context with each other; for example, being able to analyse phone calls, emails, chat messages and trades between a group of individuals together enables accurate event sequences and conclusions to be drawn, which could be missed if the different forms of data are reviewed in different systems by different people.

V INVESTIGATING DATA

Understanding and utilising structured and unstructured data has become the lynchpin in advancing large, complex investigations. The escalation of volume and types of electronic information has made sifting through and contextualising information a significant challenge in all types of investigations.

When dealing with data during an investigation, there are really two different perspectives through which to analyse it: content and forensic technology.

From a content perspective, the investigation will be focused on the actual content contained within the data or documents in question – what was ‘said’, to whom and when. Typically this is referred to as a ‘document review’ exercise, which comprises two stages, although as I will explain later, there are many different analytical methods that can be applied to arm and inform the investigator.

The first stage of a document review, often called the early case assessment, refers to the steps followed to search and filter the processed documents in order to create a review population (i.e., a population of documents that will then be reviewed). Typically, this will involve a series of evolving searches and filters based on the investigation team’s knowledge of the case, associated facts, hypotheses and lines of enquiry. It is especially important in the context of an investigation to consider this a ‘living’ process, so that it lives symbiotically with the investigation, evolving as the investigation as a whole does.

The second step relates to the actual substantive review of the documents. Typically, this is performed using a web-based review system, which enables the reviewers to see the documents, tag them based on a predefined schema and make comments on them because they are relevant to the investigation. In most cases, documents will pass through several review phases, until all of them have been reviewed and tagged appropriately. During this process, the findings from the review will be integrated with the rest of the investigation, ensuring that they form part of the overall strategy and report.

However, technology can assist beyond providing a platform to search, review and code documents based on their content alone. By analysing either the metadata related to a document or by analysing the documents through lenses other than the keywords they contain, greater insights can sometimes be gained from the review. These processes never remove the need to review the actual document, but they do provide more context or linkages around the documents and their potential relevance to the investigation.

There are a variety of different lenses that can be applied across the data. Their applicability to an investigation will vary depending on the data itself and the nature of the investigation. Some of the most common methods are detailed below.
i  **Time analysis**  
Rather than focusing on what was said, this process focuses on when something was said, almost irrespective of what was actually said. This enables the investigator to see the entire pattern of communication around critical time periods, rather than only those that contain a key word, and enables themes or issues to be ‘mapped’ over time.

ii  **Network analysis**  
Rather than focusing on what was said, this process focuses on who said something, almost irrespective of what was actually said. This enables the investigator to focus on communications or interactions between key people relevant to an investigation and gain a view of their relationship. This can specifically help to identify:

- the relationships between key players in an investigation, between individuals and among the group;
- hidden relationships with additional players who were previously unknown to the investigation team; and
- the flow of money or information between players in the investigation.

iii  **Entity extraction**  
This seeks to automatically identify known entities (e.g., people, places, organisations, times, things) from within all the documents in the repository. Any identified entities can then be searched and analysed as part of the investigation. This can not only help identify formerly unknown entities but can also help to establish the links and relationships between different entities within the investigation.

iv  **Clustering**  
The system uses the results of the semantic index to cluster like documents together based on their key concepts and terms, as opposed to anything else. This process can also take into account other variables, such as dates or times and participants in a conversation. This allows for documents to be viewed through the overall context of their meaning as opposed to the actual words used. This process can be used in various ways:

- examining the entire population at a high level to get a ‘feel’ for the overall content and what the key topics are;
- quickly removing irrelevant or trivial content from the scope of the investigation; and
- finding conceptually similar documents to a particularly key document that has been identified through other means.

v  **Sentiment analysis**  
The content of a document is analysed to determine, if possible, whether it is projecting a positive, neutral or negative view. This enables an investigator to potentially focus on key conflict documents by analysing those with a particularly negative sentiment. A similar analysis can be performed to determine whether the content of a document is considered subjective or objective.
Two additional analyses can be applied to the results from some or all the above lenses, the first being that multiple lenses can be applied in conjunction with each other, thereby building more complex analytical queries; for example, search for all communications between A and B that are negative in context and include the entity ABC Limited. These can also be combined with traditional filtering and keyword searches to provide a much more comprehensive and sophisticated analytical toolbox for the investigator.

The second relates to the way that the results are displayed and the use of visualisations to aid the investigator. This lends itself to the fact that, generally, human beings can take in more information and see patterns more readily if in graphical form, rather than a long string of text. These exist in all sorts of different shapes and sizes and can focus on content (for example, a word cloud) or on a particular item of metadata (for example, a geographical representation of search results).

VI FORENSIC DATA INVESTIGATION

As well as considering documents and data from a content perspective, a parallel line of investigation relates to the forensic aspects of the data. This generally relates to how the relevant individuals used technology and what they did, as opposed to the live content contained within. Therefore, this line of investigation is generally focused on sources that individuals ‘touch’ (i.e., physical and personal devices such as computers, smartphones, tablets, USB drives) as opposed to remote storage-central systems. There are some exceptions, such as:

a where the company uses virtual machines to run their operations, these will generally be stored remotely and need to be investigated in the same way as a physical device would be; it is just collected from a different source; and

b when considering deleted files, deletion exercises are not necessarily limited to physical devices and can be performed across networked drives and email systems; however, the best form of attack to counter this is to include backup tapes in the investigation through a ‘content perspective’ as opposed to dealing with them forensically. Additional analyses would probably be performed looking explicitly at what and when data was deleted.

The list of forensic techniques that can be applied across systems is very long; however, I will focus on the most common, and on the most common subject of a forensic investigation: a Windows-based computer.

The first technique that is core to most investigations is the recovery of deleted files. This is based on the fact that where there is malpractice, people tend to try to cover their tracks and deleting files is one way of attempting to do this. Although it is always best to start an investigation without the suspects being aware or suspicious of an investigation, this is not always possible; therefore recovering deleted files is a key step to take in an investigation.

Before examining deleted files, it is important to explain some of the technological workings of a Windows-based computer so that the process can be fully understood.

A partition (or a logical volume) on a computer hard drive is a single storage area with a single file system that can have data written to it and is generally referred to by a letter followed by a colon and a back-slash (e.g., C:). The new technology file system (NTFS) is the one used by Microsoft in its operating systems, since the introduction of Microsoft Windows NT, to manage all files and folders on the partition (including itself). Fundamentally, the NTFS works by viewing a partition
as having two main components, an index component and a data component. The index component, which is called the master file table (MFT), contains a list of the files and folders contained on the partition, details about them and pointers to the location of files in the data component. The data component contains the actual data of the files and its usage is managed by system files, including the $bitmap file. Every file and folder has a separate, unique entry in the MFT.

The Recycle Bin is a special folder that Windows uses as a repository for files that are deleted in a normal manner from a fixed drive (e.g., a hard drive). Generally, there is a Recycle Bin for each user on each partition of a drive. Files and folders that are deleted in a normal manner from a fixed drive are moved by the operating system to this folder and renamed. There is also a database system within each Recycle Bin that records the original location of the deleted files or folders and the time and date they were deleted.

When a user deletes a file, it does not mysteriously disappear from a computer. The first thing that happens is that it is moved to the Recycle Bin (see above for how this operates). The next phase of a ‘deletion’ is when the user empties the Recycle Bin. What this actually does is delete the renamed file and empties the associated database within the Recycle Bin. In respect of it ‘deleting the renamed file’, effectively two things happen:

a. The flag in the file’s MFT entry is changed to say it has been deleted, and that the operating system can reuse that entry in the MFT.

b. The operating system is notified that it can reuse the space where the file was saved (e.g., to act as though the file was not there) through a special ‘file’ called the bitmap, which tracks which areas of the disk are used and which are not. It does not change anything in respect of the file content itself.

However, at this point both the MFT entry and the space on the drive where the file was saved are perceived as being ‘free’ by the computer and hence new data can, and given enough time, probably will be saved in their place, thus overwriting the previous contents. This does not necessarily happen in a totally predictable or timely way. In respect of the MFT, Windows will always use the first available entry when writing a new entry in the MFT, but in respect of the drive space, there are no known rules or logic to explain when or if the data will be overwritten and whether the overwriting file will overwrite all or some of the previous file. Therefore, there are a number of resultant possibilities that can occur, as set out in the table below:

Table 2: Different stages of file deletion and the associated consequences for recovery

<table>
<thead>
<tr>
<th>MFT entry</th>
<th>Data area</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not overwritten</td>
<td>Not overwritten</td>
<td>The file can be fully recovered and all details about it are available</td>
</tr>
<tr>
<td>Overwritten</td>
<td>Not overwritten</td>
<td>File content is recoverable but no details about the file are known (e.g., name, dates, etc.)</td>
</tr>
<tr>
<td>Not overwritten</td>
<td>Partially overwritten</td>
<td>Details of the file are available, but only a fraction of the content is available (it is not recoverable and needs to be viewed using specialist forensic software)</td>
</tr>
<tr>
<td>Not overwritten</td>
<td>Fully overwritten</td>
<td>Details of the file are available, but no content is available</td>
</tr>
<tr>
<td>Overwritten</td>
<td>Partially overwritten</td>
<td>Fragments of unassociated text are available (i.e., you may be able to locate interesting text but you will not be able to determine which file it originated from or anything about it)</td>
</tr>
<tr>
<td>Overwritten</td>
<td>Fully overwritten</td>
<td>Nothing is recoverable</td>
</tr>
</tbody>
</table>
From an investigation perspective, where the data area has not been overwritten, files should be recovered and be included in the subsequent processes along with the other data relevant to the investigation. Where the MFT entry is not overwritten but the content is, then this information alone can be relevant and should be incorporated into the investigation.

An extreme case of deletion is when a user ‘wipes’ data from a computer. There are numerous free tools available that enable users to do this fairly easily, although it can take significant time to fully wipe data and the tools will only wipe what they are instructed to; some relevant materials can therefore sometimes be missed from this process. Effectively what wiping does is to purposefully overwrite the specified areas of the hard drive with random data, thus making the previous content unrecoverable. However, from an investigation sense, although the content may be lost (from this source), there are relevant findings that can sometimes be established to be incorporated into the investigation, such as:

a. the fact that wiping has occurred;
b. a time frame of when the wiping is likely to have occurred; and
c. details of what was wiped.

Two other key techniques often used as part of an investigation are analysing internet activity and profiling other user-related activity on the computer. Although they sound similar, the areas of a computer that are analysed to produce the analysis are very different.

In respect to internet activity, although every browser works in a slightly different way, there are in principle three sources of evidence that can be analysed to help determine usage:

a. the cache: this records local copies of the content reviewed during a browsing session, including web pages, graphics and other components from the web pages;
b. the history: this is a database that tracks the websites visited during a browsing session and various metadata related to the pages; and
c. other related files, such as cookies: these are used in various ways by different applications to track or ‘improve’ the way the application works.

By analysing these together, including deleted versions that can sometimes be recovered in the same way as any other data, it is possible to produce a detailed picture of how the internet was used on the computer. This can be of upmost importance and relevance to an investigation, for example where relevant content can be identified and recovered from:

a. personal web-based email systems;
b. web-based or cloud storage systems;
c. search histories; and
d. a general review of websites visited.

In respect to profiling the user activity on a computer, the most important source of evidence is the registry on a Windows computer. The registry is a large database, made up of various individual files, that manages the different components, software and users on a computer and how they all interact with each other. It is used extensively by the operating system and all applications installed to ensure that they perform in the way that they are intended. In respect to investigations, there are a number of key facts that can be determined from analysing the registry that should be incorporated into the wider investigation, which include:

a. recently used files and folders;
b. other external devices (e.g., USB devices) that have been used in connection with the computer;
c. time and date settings on the computer;
network drives that have been used;

log-on and log-out times for users; and

Wi-Fi networks that have been connected to.

In addition to the techniques referred to above, there are many others that can significantly aid an investigation and, given the right circumstances, should be central to the process.

VII USE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING TO SUPPORT INVESTIGATORS

All the aforementioned investigatory tasks and steps involve a human being making the lead decisions and instructing a computer to perform analyses. However, computers can aid an investigation by having a more active role in deciding the direction of the investigation, or making it more efficient through the use of artificial intelligence and machine learning. There are four specific uses of these techniques that can be especially applicable to investigations: predictive coding, predictive analytics, link analysis and in-context searching and analysis.

Predictive coding, also known as predictive text analytics or technology-assisted review, uses a combination of statistical analysis and computer-learning algorithms to make the document review process more efficient. It allows for the system to automatically propagate coding decisions across the entire population of documents, based on how a human being codes an initial sample or samples. This is an approach that is commonly used in disclosure review exercises, but can be less relevant in an investigation (except maybe in the closing stages when the fact base is more complete) as the fact base is not necessarily known and, therefore, what is relevant to an investigation will change over time as the fact base will also change as the investigation progresses. One specific use is a ‘find similar’-type search around specific key documents, whereby the system will identify other documents that, based on the same statistical analysis and computer-learning algorithms, are similar to the key documents already identified. Another use of predictive coding is as a form of quality control to ensure that no documents similar to those identified as being key to the investigation have been overlooked.

Predictive analytics is very similar to predictive coding in concept but is applied across structured data as opposed to unstructured textual data. Effectively it is the practice of using advanced statistics and historical data to predict future outcomes, and applies a very similar approach to the above, namely:

a the identification of relevant historical datasets, referred to as training data, where the outcome to be predicted is known;

b the application of machine learning algorithms to identify patterns or relationships within the data that have a high probability of predicting an outcome;

c these models, once tested and refined are used to create a model; and

d that model is applied to either the remainder of the dataset or new data as it becomes available to predict the outcome.

Link analysis takes the concept of entity extraction, discussed above, a stage further, and as well as identifying the entities contained within a document, it identifies relationships between them. These relationships can be both assessed by a human being to determine their strength and relevance, and strengthened based on multiple occurrences of the same identification across multiple, non-duplicate, documents. This then enables these relationships to be automatically mapped within a visual chart to depict them and how
different relationships relate to each other, eventually generating an overall relationship analysis diagram, as is commonly used within an investigation, the key difference being that in using this technology, they are automatically identified.

The final concept is one that enables in-context searching and analysis. This is where the system prompts and promotes lines of enquiry that investigators might wish to take based on an analysis of a combination of the data population and the action taken by the investigator. The system effectively learns what sort of action generates relevant documents (based on human actions and decisions) and then seeks to augment the investigation through making likely relevant suggestions.

The technologies for this are not being developed in a legal or investigative context but rather in a wider machine-learning context and most of them can be readily observed in the way large technology companies, such as Google, Facebook, Amazon, Apple and Microsoft, use them to enhance web browsing or online behaviour.

**VIII CONCLUSION**

Technology will never replace human beings within an investigation but it will enable them to understand, connect and analyse more data from different sources in a single environment. Therefore, it is essential when undertaking an investigation that, not only is the full scope of data considered within the investigation, but also that the technology is used to its fullest extent to enhance and drive efficiencies within the investigation.

When approaching an investigation, there are five key points that must be fully considered:

1. ensure that all data is collected in a forensically sound manner to avoid any issues with its future admissibility and use;
2. document all actions and decisions taken throughout the investigation to ensure that the process is managed efficiently and effectively;
3. ensure that all processes are verified and confirmed to ensure that the full set of data is included in the investigation and nothing has been missed;
4. fully incorporate the investigation of data into the overall investigation to maximise its benefit; and
5. ensure that the work is performed by a qualified expert.
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.

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).

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.

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.

1 Stefaan Loosveld is a partner at Linklaters.
2 Commission Notice on immunity from fines and reduction of fines in cartel cases (OJ C 298, 8 December 2006, p. 17).
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 that enables 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, 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 from 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

At the EU level, various pieces of legislation in the areas of financial services generally and banking specifically contain rules on the establishment of mechanisms for the reporting of infringements, commonly known as whistle-blowing. These mechanisms 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 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;

---


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

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 to say, 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 everybody that 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.

---


12 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 Directive IV (CRD 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.
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. 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 authority over ‘significant institutions’. To ensure compliance with the supervisory rules and its regulations and decisions in this area, the ECB has significant supervisory, 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 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 breaches, intentionally or negligently, 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

---

14 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.
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.

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 in order 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 and for judicial reviews.

---

17 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.

18 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.

Chapter 4

AUSTRALIA

Dennis Miralis and Phillip Gibson

I

INTRODUCTION

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

- The Australian Securities and Investments Commission (ASIC) is the main corporate regulator. It enforces and regulates company law.
- The Australian Competition and Consumer Commission (ACCC) enforces and regulates competition and consumer laws.
- The Australian Tax Office enforces and administers the federal taxation system and superannuation law. It is Australia's principal revenue collection agency.
- 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.

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:\(^2\)

\[\begin{align*}
a & \quad \text{fully recognise that cooperation (taking into account whether the corporate has a self-reporting obligation);} \\
b & \quad \text{negotiate alternative resolutions to the matter;}
\end{align*}\]

\[\begin{align*}
c & \quad \text{take into account the degree of cooperation provided during the investigation when determining the type of remedy or remedies sought, depending on all the circumstances of the case;}
\end{align*}\]

\[\begin{align*}
d & \quad \text{in administrative and civil matters (other than civil penalty matters), make particular submissions to the tribunal or court as to what the outcome should be;}
\end{align*}\]

\[\begin{align*}
e & \quad \text{in civil penalty matters, take the corporate’s cooperation into account; and}
\end{align*}\]

\[\begin{align*}
f & \quad \text{in criminal matters, take the corporate’s cooperation into account.}
\end{align*}\]

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:\(^4\)

\[\begin{align*}
a & \quad \text{proactively identify and address wrongdoing within the company;}
\end{align*}\]

\[\begin{align*}
b & \quad \text{comply with directors’ statutory and fiduciary duties to act in the best interests of the company;}
\end{align*}\]

\[\begin{align*}
c & \quad \text{limit corporate criminal liability;}
\end{align*}\]

\[\begin{align*}
d & \quad \text{minimise reputational damage;}
\end{align*}\]

\[\begin{align*}
e & \quad \text{demonstrate a cooperative intent with the AFP in investigating the conduct;}
\end{align*}\]

\[\begin{align*}
f & \quad \text{maximise the sentencing discount that will be available to the company in any relevant prosecution of the company; and}
\end{align*}\]

\[\begin{align*}
g & \quad \text{be a good ‘corporate citizen’}. \\
\end{align*}\]

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

\(^2\) 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.

© 2018 Law Business Research Ltd

26
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:\(^6\)

\[ \text{a} \] improving the potential for detecting foreign bribery through Australia’s anti-money laundering system;

\[ \text{b} \] enhancing whistle-blower protection for private sector employees;

\[ \text{c} \] continuing to investigate and prosecute foreign bribery and ensuring appropriate resourcing of authorities to facilitate those improvements; and

\[ \text{d} \] engaging with the private sector to encourage adoption of robust anti-bribery procedures.

With the anticipated introduction of deferred prosecution agreements (DPAs), Australia’s enforcement landscape regarding foreign bribery will become more aligned with international developments in the United Kingdom and the United States, where self-reporting and the resolution of matters through sentencing alternatives for corporations other than criminal sanctions, remains an important part of the sentencing options available to government and the courts.

\[ \text{ii} \] 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 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 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 be undertaken in order to comply with a relevant law,

\(^5\) Ibid.

\(^6\) Implementing the OECD Anti-Bribery Convention Phase 4 Report: Australia.
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 failing to investigate, delay and inactivity.

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 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, in the event that 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. 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. 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).

---

7 Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters.
8 See https://ogpau.pmc.gov.au/.
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 proposed 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.

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 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 proposed 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. The amendments are comparable to the proposed amendments to the Corporations Act 2001 (Cth), namely, 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 a mechanism for court-awarded compensation to persons who suffer damage in respect of a qualifying disclosure.

If passed, the Treasury Laws Amendment (Whistleblowers) Bill 2017 (Cth) will apply to whistle-blower disclosures made on or after 1 July 2018. 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.

III ENFORCEMENT

i Corporate liability

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.

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). The government has agreed in principle to this recommendation. Additionally, it has been recommended that the ASIC be provided with similar powers to the AFP and be directly able to freeze and forfeit proceeds of crime.

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.

### 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.

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.

### 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.9 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.10

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.11 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.12

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.13 However, there are some restrictions on the extent to which the ASIC can provide assistance to foreign authorities. Sections 6 and 7

9 Part 5B, Division 2, Corporations Act 2001 (Cth).
10 Section 206H, Corporations Act 2001 (Cth).
11 Division 14, Criminal Code 1995 (Cth).
12 Division 15; Criminal Code 1995 (Cth).
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.

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 in order 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.

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

There has been a number of high-profile cases 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 *R v. Raines* [2017] NSWDC 217, the defendant was sentenced after pleading guilty to two counts of conspiracy to falsify books relating to the affairs of a corporation in contravention of Section 1307(1) of the Corporations Act 2001 (Cth) and one count of conspiracy to knowingly make false information available to an auditor of a corporation contrary to Section 1309(1) of the Corporations Act 2001 (Cth) and Section 11.5(1) of the Criminal Code.

The offences occurred between 7 November 2008 and 30 June 2011 and concerned the falsification of financial records of Hastie Services Pty Ltd. The offences were engaged in with three other employees, including the chief executive officer, the general manager and the finance manager of Hastie Services. The defendant was the chief financial officer of Hastie Services, a public company that provided technical installation and maintenance of smaller-scale fit-outs for commercial air-conditioning systems.

The conspiracy in relation to all offences was discussed in person and via email. The matters taken into account on sentence was that the offending was objectively serious, was committed by a senior employee in a position of trust and responsibility, that the conduct was persistent and deliberate, that the defendant had shown a significant degree of contrition, that the offender was willing to provide future assistance and had prior good character.

The terms of imprisonment, after a 50 per cent discount, were nine months for the first offence, eight months for the second offence, and one year six months for the third offence. The defendant was referred to Community Corrections to be assessed for a community sentencing option.

*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 agrees 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).

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.

This includes the new anti-money laundering and counterterrorism financing laws that have just 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 counterterrorism 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

© 2018 Law Business Research Ltd
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 by 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.
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 to question witnesses, for example. 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 others.

After the investigation procedure has been completed, the public prosecution 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 and 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. Shortly after taking office in 2013, the acting Federal Minister

---

1 Norbert Wess is a partner, Vanessa McAllister and Markus Machan are associates at wkk law Rechtsanwälte, Attorneys at Law.
of Justice supported the idea of an abolition of the right to issue instructions to subordinate prosecutors. A commission of experts has been set up to make a proposal concerning each single case that is reported to the Minister.

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


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.
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 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 BWB is entitled to request the imposition of 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 investigation 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 (i.e., 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 counsel 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 (Hg), Wirtschaftstrafrecht und Organverantwortlichkeit Jahrbuch 2013 (2013) 271.
Austria

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.

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, 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 year of its existence, more than 1,200 tip-offs had been registered, only 6 per cent of which were dismissed as being unsubstantiated. 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, 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 in order to prevent such an offence. The employee himself or herself 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.

---

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 amount of daily rates. 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 one 360th part of the corporation’s annual yield (this amount may be exceeded or fall below by one-third). The maximum amount of a daily rate, irrespective of the corporation’s economic performance, is €10,000.

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 in order 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 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 not unlikely 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.

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.
ii 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 case of intentional offences and 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 or of 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 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.

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 bank 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. 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

a The Austrian Criminal Code was partially reformed in 2017. By means of the amendment that came into force on 1 September 2017 (Strafgesetznovelle 2017), existing criminal offences have been adapted, tightened up or eased, and some new criminal offences have been introduced, mainly to counteract certain social phenomena and developments of recent years.

b In the implementation of Directive 2015/149/EU (the Fourth Money Laundering Directive), Article 165 of the Austrian Criminal Code was modified. The list of predicate offences has been expanded and now includes all criminal offences with threatened imprisonment of more than one year. Money laundering is no longer limited to crimes against property any more. As a result, most financial offences are now also covered. However, the extent to which financial offences can produce assets within the meaning of Article 165 Austrian Criminal Code is controversial. According to prevailing opinion, only financial offences that are under the jurisdiction of the courts can be predicate offences of Article 165 of the Austrian Criminal Code. Tax savings (unlike tax credits and refunds) are not assets. However, fees and bonus payments received by participants of a criminal offence are subject to the predicate offence.

c With regard to the law on legitimate self-defence pursuant to Article 3 of the Austrian Criminal Code, the amendment of 2017 adds to the legally protected rights already mentioned in Article 3(1) (life, health, physical integrity, liberty and property) those of sexual integrity and self-determination. As a result of this legal recognition of further legally protected rights, it is now ensured that a person who is being sexually harassed can carry out justified self-defence actions against the offenders, without the necessity to check – from a legal point of view – whether other legally protected rights have been infringed.

d In response to scattered incidents in the past, criminal law relating to sexual offences (especially Article 218 of the Austrian Criminal Code) has been tightened up. According to the new criminal offence pursuant to Article 218(2a) of the Austrian Criminal Code, a person who intentionally takes part in a group intent on sexual harassment (within the meaning of Article 218(1) subparagraph 1 or Article 218(2a)) is liable to imprisonment for up to one year or a fine not exceeding 720 penalty units. Any person who agrees with at least one other person to commit the aforementioned offence is

---


liable to imprisonment for up to two years, according to Article 218(2b). Furthermore, a person who commits sexual harassment within the meaning of Article 218(1a) ('groping') by abusing their position of authority (pursuant to Article 212(1) and (2) of the Austrian Criminal Code) is now liable to imprisonment for up to one year or a fine not exceeding 720 penalty units (Article 212(3) of the Austrian Criminal Code).

The legislator sought to implement a liberalisation with regard to 'sexting'. Within the meaning of Article 207a(6) subparagraph 1 of the Austrian Criminal Code, a minor of or above the age of 14 is not liable if he or she produces and possesses a pornographic image of himself or herself and makes it available to another, as long as it has been taken at the age of 14 or older. A minor who possesses a pornographic image that has been produced before the age of criminal responsibility is not liable pursuant to Article 207a(6) subparagraph 2; distributing or sharing it with others, however, is strictly prohibited and therefore prosecuted.

Since 2014, more and more movements consisting of so-called state rejectionists have been identified. These are particularly characterised as movements or associations that, on the one hand, do not obey rules and regulations introduced by the Republic of Austria and that, on the other hand, put their own created ideologies and alleged rights and powers before those of the Austrian authorities. In fact, they strive for creation of parallel societies. Before the amendment of 2017 came into force, a participation in these movements had only been liable if acts of resistance (by use of force or threat) against a government official had taken place or other criminal offences had been committed. With the implementation of Article 247a of the Austrian Criminal Code ('subversive associations'), steps are now taken by the authorities to prevent further spread of these subversive ideologies and possible acts of violence that naturally follow. Pursuant to Article 247a(3) of the Austrian Criminal Code, a group of many individuals (according to the prevailing opinion, at least 30 people) is considered as a 'subversive association' if its main purpose manifests itself not only in fundamentally rejecting the sovereignty of the Republic of Austria (federal state, federal provinces, communities, self-governance), but also in putting its own alleged sovereignty before that of the government. A subversive association is characterised by the intention to continue its illegal actions in such a way that its manifested subversive opinion becomes obvious and prevents public authorities from enforcing laws, regulations and other sovereign decisions. According to current legislature, these actions have to take place constantly and the recognition of Austria's authority must be refused entirely; that is why refusal of various enforcement measures and resistance for certain ideologies (e.g., animal rights activists) are not liable under Article 247a of the Austrian Criminal Code. Within the meaning of Article 247a(1) of the Austrian Criminal Code, a person who establishes a subversive association or participates in one in a leading capacity is liable to imprisonment for up to two years. Mere participation is only liable if the offender also has the intention to support and promote the association in its subversive ideology (e.g., by providing considerable financial means) and if his or her intention is objectively put into action pursuant to Article 247a(2). However, the newly introduced criminal offences under Article 247a of the Austrian Criminal Code can only be applied if the committed criminal acts are not already subject to stricter penalties (subsidiarity in criminal law – Article 247a(4) of the Austrian Criminal Code). On the other hand,

9 Flora in SbgK Section 193 Rz 93.
a person is not liable if he or she resigns noticeably from a subversive association before public authorities become aware of the person’s culpability (active repentance – Article 247a(5) Austrian Criminal Code).

To prevent increasing aggressive behaviour towards the authority of the State, a person who violently attacks a government official during the execution of an official act pursuant to Article 269(3) of the Austrian Criminal Code is now liable to imprisonment for up to two years (Article 270 of the Austrian Criminal Code).

VI CONCLUSIONS AND OUTLOOK

Despite the last, rather comprehensive, amendment to the Austrian Criminal Code (which came into effect in 2016), a new amendment to the Austrian Criminal Code is planned for 2018. The main changes, however, focus (again) on violent crime and sexual offences.

The new government programme for 2018–2022 provides far-reaching revisions and reforms in many areas of criminal law and criminal procedural law. However, at the moment this is more a declaration of intent than an amendment plan. Concrete reforms are currently unknown.
Chapter 6

BELGIUM

Stefaan Loosveld

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 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) and the financial and banking regulators (which supervise, investigate and sanction the conduct and activities of financial services providers, including banks).

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:
  •  the actions and measures taken by these regulators remain within the confines of what they are legally entitled to do; and

---

1  Stefaan Loosveld is a partner at Linklaters. The content of this chapter is accurate as at July 2017.
• 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. 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.

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

---


3 Commission Notice on Immunity from fines and reduction of fines in cartel cases (OJ C 298, 8 December 2006, p. 17).
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 in order 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 2016.4 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.5 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.

Under the Antitrust Damages Directive,6 soon to be implemented in Belgian law,7 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 will also facilitate disclosure of evidence. However, leniency statements at both the EU and Belgian levels are shielded from requests from 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

---

4 Guidelines on Leniency Notice on full or partial immunity from fines in cartel cases (Belgian Official State Gazette, 22 April 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.
7 As at mid May 2017, draft legislation implementing the Antitrust Damages Directive in Belgium was pending before the Belgian Parliament.
Belgium

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.

ii 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.

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 others, 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.

iii Whistle-blowers

EU financial services and banking

At the EU level, various legislation in the areas of financial services generally and banking specifically contains rules on the establishment of mechanisms for the reporting of infringements, commonly known as whistle-blowing. These mechanisms 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 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:

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

---

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 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, undertakings for collective investment in transferable securities (UCITS), insurance distribution, and packaged retail and insurance-based investment products (PRIIPs).

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. 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 ‘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.\footnote{In full: Regulation (EU) No. 468/2014 of the European Central Bank of 16 April 2014 establishing the framework for cooperation within the Single Supervisory Mechanism between the European Central Bank and national competent authorities and with national designated authorities (ECB/2014/17) (OJ L 141, 14 May 2014, p. 1).}

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).\footnote{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 (CRR). 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 Directive IV (CRD 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.} If a breach relates to other areas of activities of 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 (e.g., the Economic Inspection for consumer protection, including when it applies to the activities and conduct of credit institutions). 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. 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 that 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. 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.
Belgium

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

Belgian law does not contain general rules on whistle-blowing. However, particularly in relation to financial services and banking, either Belgian law has already implemented the relevant EU legislation or this legislation is in the process of being implemented.

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. 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. It governs, among others, the good faith reporting to the NBB of an actual or potential 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.

As at June 2017, draft legislation was being finalised for adoption by the Belgian Parliament. This will implement 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. This legislation will modify the Belgian Law of 2 August 2002 on the supervision of the financial sector and the financial services. The rules governing the ‘external’ dimension of such mechanisms will be addressed in a new Article 69 bis of this law – with the Belgian Financial Services and Markets Authority (FSMA) functioning as the authority to whom the reporting will need to be done – while the ‘internal dimension’ is laid out in a new Article 69 ter.

Importantly, these new provisions will not be limited to implementing into Belgian law the requirements of the EU legislation, but will 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 so-called ‘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 new whistle-blowing provisions will 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.

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.

In full: Law of 25 April 2014 on the status and supervision of credit institutions.
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. That is the first time that whistle-blowing will be rewarded under Belgian competition law.

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 the European Commission will exactly calculate the fines. 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. First, the maximum amount of the fine is 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). The Belgian Competition Authority (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. 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.

There are no criminal sanctions under Belgian law for competition law infringements.

---


19 An amendment of this rule, in order to calculate the maximum amount of the fine on the basis of the worldwide turnover of the undertakings concerned, is being discussed as part of a package of reforms to Belgian competition legislation.

20 Belgian Official State Gazette, 10 September 2014, p. 71456.

21 Some exceptions apply, e.g., bid rigging in public procurement and breaking of seals applied by the BCA.
**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, 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 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 breaches, intentionally or negligently, 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 the case of breaches of regulations or decisions adopted by the ECB in the exercise of its supervisory tasks. The ECB also has the right to publish the imposition of such sanctions, irrespective of whether the decision has been appealed.

---

22 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.


25 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.

26 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.
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, which, among others, sets forth the procedural rules and time limits for the imposition of sanctions, as well as their judicial review.

At the level of the Member States (the NBB in Belgium, for instance), has the use 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 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.

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, as well as in the provisions of an internal regulation from the Sanctions Commission of the FSMA of 21 November 2011.

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, injunctions to perform certain activities, 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, which only provide that the BCA may take into account

---


any initiative of the undertaking aimed at avoiding competition law infringements. It is, nonetheless, highly recommended for undertakings to implement competition law compliance programmes, since 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 facts (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).

29 Fining Guidelines, paragraph 41.
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. 1/2003.30 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.

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.

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 has been 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.

I  INTRODUCTION

Brazilian criminal procedure law establishes that investigation of the origins and content of crimes committed within or by companies may be carried out by federal and state civil police forces.² It is also possible that the Public Prosecutor’s Office (at state and federal levels) will carry out its own investigation.³ 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, as far as the conduct of these authorities respect 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. 8,420/2015, which regulates the Brazilian Anticorruption Law (Law No. 12,846/2013), 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 relevant authority may determine the commencement of the administrative procedure⁴ by which any sanctions on the entity under investigation will be established. A finding of guilt is always subject to judicial review.

Private agencies and investigators, even though they are authorised to operate in Brazil, 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,⁵ as long as the evidence has

---

¹ João Daniel Rassi and Gauthama C C Fornaciari de Paula are partners and Victor Labate is an associate 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. 8,420/2015.
⁵ Article 5 of Law No. 13,432/2017.
been obtained within the tenets of the law. Pursuant to Law No. 13,432/17, companies and individuals are legally allowed to cooperate with the authorities by providing evidence gathered as part of an internal investigation.

II CONDUCT

i Self-reporting

As a rule, private companies are not required to report irregularities 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 obligated are individuals and legal entities that – permanently or occasionally, principally 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).

Other laws also allow for leniency, called 'rewarded denunciation'. 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).

---

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 (1) warning, (2) fine, (3) temporary ineligibility to hold management positions and (4) cancellation or suspension of authorisation to engage in activity, operation or functioning.
11 Article 1, Section 5 of Law No. 9,613/98.
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).
13 It was through rewarded collaboration of this nature that Operation Car Wash, the biggest investigation Brazil has ever seen of corruption and money laundering involving important executives, was successful.
In the area of antitrust law, the forming of a cartel is both an administrative\(^{14}\) and a criminal\(^{15}\) 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, under the leniency programme established in Article 86 of Law No. 12,529/11. That programme is made operational by the signing of a consent decree between a member of the cartel or individuals involved in its operation and the Administrative Council for Economic Defence, the antitrust agency, in return for cooperation in identifying and producing evidence against the other participants.\(^{16}\)

With respect to the criminal sphere, Article 87 of Law No. 12,529/11 establishes that the consent decree prevents charges being brought against the 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,\(^{17}\) such as fraud in public tenders (Article 90 of Law No. 8,666/93) and criminal conspiracy (Article 288 of the Penal Code).\(^{18}\) Upon compliance with the obligations assumed in the consent decree, the competent criminal judge will declare that the person is not eligible for punishment (Article 87 of Law No. 12,529/11).

The granting of such benefits by the authorities responsible for establishing the collaboration agreement and the leniency programme are subject to the authorities' subject valuation. The lack of objective parameters is often criticised by legal entities.\(^{19}\)

**ii Internal investigations**

Companies that receive denunciations of or suspect their employees of irregular acts can conduct their own investigations to identify the behaviour and impose penalties on those found responsible.\(^{20}\) They can also engage external advisers, private detectives or audit firms to conduct investigations. As a rule, the investigation should involve as few people as possible

---

\(^{14}\) 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.

\(^{15}\) Article 4 of Law No. 8,137/90.

\(^{16}\) There is also the benefit called a cease and desist agreement (TCC), related to the practice under investigation or its harmful effects. According to Article 85 of the Brazilian Competition Law, the TCC should contain the following elements: (1) the specification of the defendant's obligations not to practise the investigated activity or its harmful effects, as well as obligations deemed applicable; (2) the settlement of the fine to be paid in case of failure to comply, in full or in part, with the undertaken obligations; and (3) the settlement of the pecuniary contribution to be paid to the Diffuse Rights Defence Fund, whenever applicable. The act of signing a TCC grants no benefits in the criminal area, such as a lighter penalty, no criminal action, suspension of the time bar, etc. This will only happen in the leniency agreement.

\(^{17}\) In its last Peer Review on Competition Law and Policy in Brazil, the OECD recommended modification of the leniency programme to eliminate the exposure of leniency participants to prosecution under criminal laws other than the Economic Crimes Law.

\(^{18}\) Concerning non-related crimes, it is possible for the defence to request the diminishing of criminal penalty for confession under Article 65, III 4) of the Brazilian Penal Code.


to protect the person making the accusation, the accused individual or individuals and to
preserve the investigation itself. For this purpose, all those involved are typically asked to sign
a confidentiality undertaking.\footnote{Ibid, pp. 98 to 101.}

Audit reports, spreadsheets, official emails\footnote{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.} 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, these kind of investigations are conducted by external counsel, or by internal counsel assisted by external professionals, to ensure that the impartiality of proceedings is not affected. 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.\footnote{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).} 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, since 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.

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.\footnote{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).}

Despite the fact that Decree No. 8,420/2014 determines that companies can create internal channels to enable denunciation of irregularities, for which benefits may be used as reward, the Brazilian legal system does not provide any specific mechanism to protect whistle-blowers.\footnote{D M Cardoso, A extensão do compliance no Direito Penal: análise crítica na perspectiva da Lei de Lavagem de Dinheiro, Faculdade de Direito USP: São Paulo, 2013, p. 66.} There are also no provisions on administrative penalties or punishments for those who make denunciations in bad faith or that are knowingly false,\footnote{On this aspect, the Brazilian Penal Code, in Articles 138 to 140, defines the crimes of calumny (falsely accusing someone of a criminal offence), defamation (harming someone's reputation by false accusations)
However, if a whistle-blower suffers a backlash as a result of making a denunciation, such as dismissal or mental harassment, he or she can file a labour suit against the company.\(^\text{27}\)

### 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: (1) by reason of *culpa in eligendo* (poor choice of those entrusted with performance of obligations); (2) by reason of *culpa in vigilando* (insufficient oversight of the performance of obligations); and (3) 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*\(^\text{28}\) 341 from the Federal Supreme Court.\(^\text{29}\) 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 injurious to national or foreign public administration.\(^\text{30}\)

Civil and administrative corporate liability under this provision does not preclude the personal liability of the individuals involved in such conduct.\(^\text{31}\)

Criminally, only companies can be held liable for the commission of 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 infractions 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 the possibility of a 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 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:

- 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;
- libel or slander (offending someone’s dignity or decorum with false claims). These crimes are subject to private penal action prosecuted by the offended party (as opposed to public penal actions, in which the plaintiff is the people, represented by the public prosecutor).

Labour legislation allows indirect termination of the labour contract in the situations listed in Article 483 of the Consolidated Labour Law (Decree-Law No. 5,452/43). Employees can also file suits for moral damages against acts of the employer, according to Articles 186 and 927 of the Civil Code.

---

\(^{27}\) Labour legislation allows indirect termination of the labour contract in the situations listed in Article 483 of the Consolidated Labour Law (Decree-Law No. 5,452/43). Employees can also file suits for moral damages against acts of the employer, according to Articles 186 and 927 of the Civil Code.

\(^{28}\) A *súmula* is a statement of consolidated position, or jurisprudence, from a higher court.

\(^{29}\) The culpability of the employer or principal for the acts of the employee or agent is presumed.

\(^{30}\) The list of injurious acts is contained in Article 5 of Law No. 12,846/13.

\(^{31}\) Article 3, Section 1 of Law No. 12,846/13.
Brazil

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

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

### iii 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.\(^{32}\)

The situation is different regarding civil and administrative liability for acts injurious to 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.\(^{33}\)

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

---

32 Article 6 of Law No. 9,605/98.
33 Article 7, VIII of Law No. 12,846/13.
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.34

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 job35 – even if dismissal is not mandatory for the matter in question – in case the public authorities seek to hold the individual liable or in the case of an existing investigation into that person.

On the other hand, the company can, if there is no conflict of interest, help to defend its employee 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.36

Concerning the latter situation, the possibility of extraterritorial application of Brazilian law requires that the potential injury caused by the conduct be real and effective, not just hypothetical, or there will be no configuration of a crime.37

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.38

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 or to:

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 obligated to repress owing to international treaties and conventions.39

34 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 agents entrusted with environmental vigilance and control’, circumstances that can be interpreted as resulting from the existence of a compliance programme.
35 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.
36 Article 2 of Law No. 12,259/11.
38 Article 28 of Law No. 12,846/13. See in this respect V Greco F, J D 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.
39 Article 7 of the Penal Code.
However, application of the foregoing to companies is as yet unclear, because the extraterritoriality rule was established at a time when the liability of companies for corrupt practices was not set forth in the legal system.

ii  International cooperation

The Brazilian government can cooperate with application of 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 jurisdiction. 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 Foreigner Statute (Law No. 6,815/80), Decree No. 86,715/81 and Article 22, XV of the Federal Constitution. For extradition to be granted, it is necessary for certain conditions to be fulfilled, including (1) that the act be considered a crime both in Brazil and in the requesting state, (2) that the prospective person to be extradited is a foreigner and (3) 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.

---

40 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.
42 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.
Brazilian higher courts have a consolidated approach concerning the existence of *lis alibi pendens* investigations in a sense that the closure of investigations being carried out by Brazilian public authorities may not occur under ordinary instances, provided that the admissibility test of a foreign sentence depends on analysis of the Superior Justice Tribunal. By determining the closure of the investigation, 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

Two topics are of current interest in Brazil:

- the possibility of serving provisional sentences in respect of criminal matters; and
- publication of the Orientation No. 7/2017, enacted by the 5th Chamber of Coordination and Revision of the Federal Public Prosecution Office, which establishes the minimum parameters required for the conclusion of a leniency agreement as brought under Law No. 12,846/2013.

The first derives from a prior ruling of the Supreme Federal Court that was reaffirmed on 4 April 2018, during former President Lula’s petition for a habeas corpus judgment, questioning the constitutionality of provisory sentence serving on criminal cases.

During the Lula trial, the final decision was agreed by six of the 11 judges, requiring Justice Cármen Lúcia, President of the Court, to break the tie in casting the last vote. The justices who voted against the petition argued for the necessity of an effective jurisdictional response that could only be achieved by allowing provisional sentences to be served. Some also relied on the fact that prior jurisprudence on this topic has been discussed by the court in 2016, and should be respected.

The second consists of a guide for public prosecutors who may enter into negotiation with companies and individuals willing to conclude a leniency agreement under the Anticorruption Law. The importance of this provision rests on publicising the consolidation of the parameters that have been demanded by the Federal Public Prosecution Office while concluding such agreements.

Besides the essential clauses required to conclude an agreement, an Orientation also provides the criteria used by the Federal Public Prosecution Office to estimate the applicable fees, bringing more transparency and predictability to such agreements.

---

43 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).
44 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.
45 Article 157 of the Criminal Procedure Code and Article 5, LVI of the Federal Constitution.
VI CONCLUSIONS AND OUTLOOK

The following main conclusions can be drawn.

The developments in Operation Car Wash have increased the number of companies being targeted by the investigative authorities, mainly the Federal Public Prosecutor Office and the Administrative Council for Economic Defence.

This, allied with the possibility of provisional sentencing in criminal cases, has also increased the number of collaboration agreements and leniency agreements that have been concluded with prosecution authorities. For that, the internal investigations are being consolidated as a recurrent practice for companies’ legal teams and assisting external counsels.

The recurrence of such practice is allowing the parties involved in this kind of negotiation to create a know-how, which in turn is bringing more security to companies and individuals.
INTRODUCTION

There is no overarching regulation of the investigations and proceedings dealing with the regulation and punishment of companies but there is a multiplicity of proceedings and \textit{ad hoc} configurations for each enforcement agency. An immediate consequence of this is the frequent duplication of enquiries and sanctions from agencies of the same or a broadly similar nature.

In Chile, infringements defined as ‘crimes’ by law are dealt by the Public Prosecutor’s Office, the agency that handles investigation and prosecution before criminal courts. As a principle, legal liability is strictly individual and is not applicable to collective structures such as companies, but to natural persons who have participated in the infringement. Nonetheless, an exception to the \textit{societas delinquere non potest} principle was introduced in 2009 with the enactment of Law No. 20,393, which established for the first time in Chile the criminal liability of legal persons for – at present – a limited number of crimes (bribery, money laundering, the financing of terrorism and, most recently, the felony known under Chilean law as \textit{receptación}, which punishes the individual who has, transports, buys, sells, transforms or commercialises in any way goods, knowing or having reason to believe that those goods come from the commission of other specific offences).

Alternatively, a heterogeneous range of non-criminal infringements can be found in different laws that entrust enforcement to diverse special agencies. In this group, it is relatively common for the respective agency to be entitled not only to investigate but also to impose sanctions. In contrast with criminal procedures, the civil agencies are also generally entitled to prosecute and sanction legal persons as well as individuals. These entities are usually designated as superintendencies and form part of the government (unlike the Public Prosecutor’s Office, which is an autonomous entity that does not depend on the government).

Among the most relevant active agencies in recent years are the Financial Market Commission (which this year has replaced the Superintendency of Securities and Insurance), the Internal Revenue Service in taxation issues, the National Economic Prosecutor, along with the Court for the Defence of Free Competition in antitrust matters and the Environment Agency and the environmental courts, which have been fully operative since 2013.

All these agencies are subject to different statutes and proceedings when it comes to investigating and sanctioning infringements to the laws for the areas in which they have authority; they also have different investigation powers.

\footnote{1 Jorge Bofill and Daniel Praetorius are founding partners of Bofill Escobar Abogados.}
In recent years there has been a trend to broaden special powers available to some of these agencies, as their powers have been insufficient in certain cases and are limited when compared to those available to the Public Prosecutor’s Office. For example, special powers were granted in 2009 by means of Law No. 20,361 to the National Economic Prosecutor, which has the authority, upon court approval, to execute dawn raids, seize goods and wiretap conversations. The Financial Market Commission, which replaces the Superintendency of Securities and Insurance and became operational in December 2017, has new and broader investigation powers, similar to those available to the National Economic Prosecutor, including the ability to request that bank secrecy is lifted.

Prosecution of crimes is, in general, not influenced by political agendas or domestic priorities. This is mainly due to the fact that, as already mentioned, the Public Prosecutor’s Office is an autonomous entity independent of the government. Furthermore, the National Public Prosecutor is elected by the executive, legislative and judicial branches of the state. Agencies in charge of civil enforcement have different relationships with the government, but as they have less autonomy than the Public Prosecutor’s Office, they are more vulnerable to political influence. This has led, for example, to a public discussion about the convenience of granting more autonomy to the Chilean tax authority, which has been very active during the past year in the prosecution of alleged tax fraud in connection with several prominent cases of irregular funding of political campaigns.

An interesting phenomenon regarding investigations of corporate conduct is the assumption that – particularly in certain areas – for the system to be more efficient, suspects must collaborate with agencies and find a quick remedy to the generated conflict. Evidently, as there is no legal obligation to actively collaborate, this is only relevant when the suspects have incentives to collaborate such as exemption from, or at least mitigation of, sanctions. Instruments such as leniency programmes, self-reporting and implementation of internal compliance programmes may be seen as forms of cooperation with the authorities, with underlying incentives.

The system developing from the new laws has also allowed the emergence of a broader scope for the development of efficient rights and possible judicial defences.

Individuals who are targets of prosecution by the administrative authorities or the public prosecutor have many options, not only to prove their innocence but also to find an agreed solution to the conflict.

II CONDUCT

i Self-reporting

No clear guidelines exist as to the approach that corporations should take in response to illegal or criminal behaviour. There are only a few special regulations in some areas that establish certain reporting duties.²

As a result, it cannot be stated that, as a general rule, corporations are compelled to report activities that may be prosecutable by state agencies. Nevertheless, the judicial and

² For example, in the context of money laundering, certain individuals are obliged to give notice to the authorities; however, this obligation does not apply to events occurring inside the company, but rather those performed by third parties.
legal systems are gradually providing incentives to encourage self-reporting as part of internal corporate policies. The incentives basically consist of exemption from liabilities or leniency regarding sanctions.

One example of regulations that contain incentives to encourage self-reporting can be found in Law No. 20,393, which establishes criminal liability of legal entities. According to this law, self-reporting may constitute a mitigating circumstance in the event that it is performed by the legal representatives of the company before prosecution is initiated. The law also allows the public prosecutor to enter into deferred prosecution agreements with legal entities, where the prosecution is suspended and eventually dropped if the defendant agrees to submit itself to certain conditions, such as the payment of a certain sum of money or to provide a particular service to the community.

In the field of antitrust enforcement, Chilean law considers leniency mechanisms in cases of collusion, by means of which the party coming forward can apply for a reduction and even an exemption of administrative and criminal sanctions when certain conditions are met, such as the immediate cessation of the illegal conduct and the submission of reliable and useful information that can be used by the National Economic Prosecutor’s Office as sufficient proof to file a claim before the Court for the Defence of Free Competition. A total exemption from administrative and criminal penalties is only available to the first involved party submitting its application for leniency.

The National Economic Prosecutor performs the assessment of leniency mechanisms in accordance with a procedure outlined in the Internal Guidelines on Leniency in Cartel Cases, published in March 2017, which aims to provide legal certainty to whoever wishes to obtain leniency benefits and to limit the authority’s discretion when assessing any proposals for leniency.

In environmental matters, the applicable legislation establishes benefits to encourage self-reporting, consisting of the reduction of or an exemption from applicable fines, subject to certain conditions, among them to propose and fulfil a programme to mitigate or eliminate the environmental adverse effects of the activities of the business that are in violation of environmental regulations.

Customs laws also encourage self-reporting, which, in respect of certain infringements and provided that all customs duties are paid, exempts the offender from the initiation of an administrative enforcement proceeding.

The Tax Authority has also encouraged and issued special rules for self-reporting in certain specific circumstances.

Law No. 21,000, which created the new Financial Market Commission, foresees a leniency mechanism, similar to the one that exists for cartel cases. According to this mechanism, self-reporting of infringements to securities regulations implies a reduction of up to 100 per cent of the applicable fine. The first person coming forward may benefit from a reduction of up to 100 per cent of the applicable fine in cases where more than one offender is involved, and up to 80 per cent when he or she is the sole responsible person. Subsequent offenders may only benefit from a reduction of up to 30 per cent of the applicable fine, provided they deliver important additional information on the case. As violations to securities regulations may not

---

3 In 2016, collusion was reinstated as a crime by means of Law No. 20,945. This conduct can, therefore, also be prosecuted by the Public Prosecutor’s Office in the event the National Economic Prosecutor files a criminal complaint after the administrative case has ended with the imposition of a sanction.

4 Published in the Official Gazette of Chile on 23 February 2017.
only be subject to civil enforcement by the securities supervisory authority in certain cases, but also to criminal enforcement by the Public Prosecutors’ Office, the law also provides for mitigation from criminal liability, which is only available for the first person self-reporting an infringement that also constitutes a crime. Exceptionally, the law provides an exemption from criminal responsibility if the information provided by the defendant allows specific felonies contemplated in the Law on the Securities Market to be revealed or discovered.

ii Internal investigations

Despite the development of internal investigations in terms of enforcement and judicial practice, the practice has not become widespread in Chile. The lack of legal culture in this area and the absence of precedents as to the confidentiality of findings, as well as whether they are covered by professional privilege, have led in several cases to agencies and prosecutors seizing documents produced within the scope of internal investigations. Although internal investigations conducted by outside legal counsel should be protected by privilege, it is not unusual for companies to conduct investigations internally rather than seeking assistance from outside counsel. In the absence of clear legal rules, it is arguable whether privilege covers the activities of other internal personnel, such as auditors or compliance officials. Until case law clarifies the extent of privilege in Chile, internal investigations would perhaps be better conducted by lawyers – preferably third parties – to improve protection of the confidentiality of the investigation and its findings.

Within the scope of these investigations, statements from the individuals directly involved are usually essential; however, it is important to stress that these statements must be given voluntarily by the persons involved, as they are not obliged to cooperate or submit evidence. Therefore, any participation in interviews or handing over of information must be done freely, and with the understanding that the investigation is for the benefit of the company, not for the personal defence of the individuals being interviewed or providing the information, unless the lawyer also assumes the personal defence of this person. To avoid future conflicts of interest, it should be made clear that all the information that the interviewee may provide will belong to the client (the company) and will be privileged for its exclusive benefit.

The witness may request professional legal assistance at any moment, otherwise the investigation may be invalidated.

The gathering of publicly accessible documents belonging to a company must be differentiated from documents that fall under the control or possession of a company's employee. This is particularly the case when documents or files are stored in individuals’ email accounts or computers assigned to them in the normal course of business. At least in principle, emails or documents contained within databases – even when the hard drives belong to the company – may not be accessed by the company or its counsel without the individual's consent. Furthermore, it is possible that accessing such documents without the holder's consent may expose investigators to criminal liability. However, in a ruling of February 2018, the Court of Appeals of Santiago ruled that an employer who reviewed the institutional emails of a worker, stored on a computer owned by that employer, once the worker left the company, did not commit an unlawful act, since there was a suspicion of irregular behaviour of the worker and the company reviewed the emails with the purpose of protecting business data of obligatory reserve. This case is without precedent and currently on appeal before the Supreme Court.

Finally, companies need not share or submit the results of internal investigations to the state agencies, especially when the investigation has been conducted by outside counsel.
and is privileged; however, the provision of such records may justify the mitigation of an eventual sanction, especially in the context of Law No. 20,393 (Corporate Criminal Liability Act), which recognises the amelioration of possible sanctions if the company under scrutiny improves its internal systems and compliance rules.

### iii Whistle-blowers

In the absence of almost any legal regulation, whistle-blowing is so far not a relevant issue in Chilean legal practice. Of course, it is not uncommon that in the context of enforcement actions and especially of criminal prosecution, individuals who are targets of investigations may decide to cooperate with the enforcement agency or the prosecutor to obtain more lenient treatment of their own cases. The Criminal Procedural Law allows prosecutors to enter into agreements with defendants in criminal cases, where these agreements are normally approved by the relevant criminal court. However, rather than a specific policy promoting whistle-blowing as part of the enforcement activity against corporations, this is a general statute applicable to, in principle, all criminal cases of any nature. In fact, the only limitation on these settlements is determined by law for cases where the possible sanction on the defendant exceeds five years in prison in the event of conviction.

There are no legal provisions, at least for the private sector, to protect whistle-blowers from retaliation, so the response of a company confronted with whistle-blowing by an employee will depend on its internal policies. However, since the implementation of compliance programmes has been increasingly growing in recent years, at least in large – particularly multinational – companies, it has become more common for companies to have specific whistle-blowing policies.

In the public sector, Law No. 20,205\(^5\) introduced certain provisions aiming to protect whistle-blowers who hold a public office when reporting crimes or administrative infringements to the competent authorities. However, these provisions are very limited as they only refer to certain public officers and only consider suspension of the ability to apply certain disciplinary measures against such persons for a period of up to 90 days after the investigation initiated by the report of the whistle-blower has ended. The whistle-blower may request that his or her identity and the information that he or she provides are kept confidential.

Nonetheless, the General Attorney of the Prosecutor’s Office announced recently that the Prosecutor’s Office is currently working with the Office of the Comptroller General of the Republic on a project to establish protocols and procedures to protect both public and private sector whistle-blowers regarding corruption felonies; consequently, changes in this matter are expected soon.

---

\(^5\) Law No. 20,205 of 24 July 2007, named ‘Protection to the public official who denounces irregularities and faults to the probity principle’.
III ENFORCEMENT

i Corporate liability

Corporations are generally only liable for their acts within the civil and administrative spheres. Exceptionally, they are also criminally liable when they are involved in specific acts.

The civil liability of legal entities arising from acts committed by their employees is fully recognised in civil legislation. To enforce the aforementioned, the following conditions must be fulfilled:

a in the course of committing an illegal act, harm has been inflicted on a third party;
b there is a direct cause and effect relation between the individual’s behaviour and the damage; and
c the damage is attributable to the negligence or intent of the agent.

The damage committed by the agent is attributable to the organisation of which he or she is an employee if the harm might have been prevented by the organisation had it carried out the expected level of diligence; the specific ‘degree’ of diligence that would release the organisation from liability is a matter of judicial interpretation, but there is a good chance that proper implementation of mechanisms to prevent illegal acts may lead to exemption from liability.

The administrative system of liability of legal entities is simpler. Given that the regulation specifically applies to corporations, they may be held liable. Thus, companies are subject to the sanctions that the legislation provides without requiring discussion on how the acts of the employees compromise the liability of the respective legal entities.

In connection with criminal liability, since Law No. 20,393 on Criminal Liability of Legal Entities entered into force in 2009, companies can be held criminally liable in connection with certain illegal acts committed by their agents. Hence, corporations may be investigated by the public prosecutor and be criminally sanctioned provided that:

a the illegal conduct consists of certain specific crimes defined by law;
b the illegal act is carried out by an owner, controller, representative, key officer or any person conducting managerial or supervisory functions in the company or by individuals working under the direct supervision of any of the aforementioned persons;
c the act has been performed for the direct benefit or interests of the company; and
d the behaviour of the agent or representative occurred because of a defect or failure in the company’s mechanisms of control and supervision.

In connection with the criterion in point (a), criminal liability of legal entities is restricted to certain offences committed by their agents. As a consequence, the possibility of enforcing this kind of liability is currently rather limited, but there have been and still are some attempts to broaden the scope of the offences that allow a company to be held criminally liable.

---

6 Articles 2314 et seq. of the Civil Code, particularly Article 2320.
One offence that may trigger the criminal liability of legal entities is bribery. Under Chilean law, any individual is punishable for bribery when offering or consenting to offer higher fees than those to which public officials are entitled according to their position or an economic benefit to a public official in consideration (1) of performing or having performed an action that they are obliged to do pursuant to their duties, (2) of either not performing or not having performed an action or for performing or having performed an action, in infraction of a particular duty or (3) of committing certain corruption crimes. Bribery of an international foreign official may also trigger criminal liability of a legal entity when committed by one of its agents. Commercial bribery is not a crime under Chilean law, although there is currently a Bill being discussed in Congress that aims to change this situation.

Another crime that may trigger the criminal liability of a legal entity is money laundering. The individual to be sanctioned is the person who (1) in any way hides or conceals the illicit origin of specific goods, knowing that they come, directly or indirectly, from the commission of other specific offences7 or (2) acquires, owns or uses the aforementioned goods for the purpose of profit, being aware, on their receipt, of their illicit origin. Since 2015, this offence is also punishable when committed with inexcusable negligence.

The third offence that may trigger the criminal liability of legal entities is the financing of terrorism; Chilean law punishes those who, by any means, directly or indirectly, request, collect or supply funds for the purpose of committing terrorist offences.

The fourth felony is the one known as receptación. As mentioned in Section I, Chilean law punishes an individual who has, transports, buys, sells, transforms or commercialises in any way goods, knowing (or having reason to believe) that those goods come from the commission of other specific offences.8

The fact that these offences must have occurred as a consequence of a failure or defect in the control or supervisory mechanisms in order for companies to incur liability is steering them towards effective systems of self-regulation. These are developed through prevention programmes provided in Article 4 of Law No. 20,393; the major significance of these programmes is that, even though their implementation is not mandatory, their existence and certification by entities registered in the Financial Market Commission reduces the possibility of companies’ criminal liability through a presumption of diligence, which works in their favour.

There appears to be no reason why companies and individuals cannot be defended by the same lawyer. Any conflict of interest should be resolved under the rules provided by the Bar Code of Ethics (if the lawyers are members of the Bar) or by the criminal judge pursuant to Article 105 of the Criminal Procedure Code.

---

7 The list of offences that can give rise to money laundering includes drug trafficking, bribery, use of confidential information, securities and banking frauds. Recently this list has been extended to include offences such as fraud, misappropriation, certain cases of tax fraud and piracy of intellectual property. As this increases the possibilities of application of the money laundering law, indirectly this may also lead to a greater exposure of companies to be criminally liable, as money laundering is one of the felonies that can lead to criminal liability of legal entities.

8 The list of offences that can give rise to the felony known as receptación (receiving) includes simple theft, robbery, cattle rustling and misappropriation.
The usual sanction against a company for corporate liability is a monetary fine. All administrative procedures provide a financial penalty to be applied against legal entities. The fines have gradually increased in the case of all regulations, and the trend has been adopted by state agencies such as the Superintendency of Securities and Insurance (now the Financial Market Commission), the National Economic Prosecutors’ Office and the Environment Agency, which now allow higher fines than ever before.9

Companies that require certain licences to operate or that must be registered with certain supervisory bodies may also lose their licence or be deregistered (e.g., banking). However, this kind of sanction has only been applied on very few occasions and in cases of very serious violations to sectorial regulations.

Although a fine is the usual sanction, the recent legislative changes dealing with criminal liability of legal entities have allowed the emergence of new sanctions in criminal matters. Law No. 20,393 provides that companies may be punished with the following penalties:

a. dissolution of the legal entity or cancellation of its legal status;

b. a temporary or permanent ban on entering into contracts with state entities;

c. total or partial loss of tax benefits or an absolute ban on receiving these for a certain period;

d. monetary fines; or

e. secondary penalties as described in Article 13:

- publication of details of the sentence in the Official Gazette or any other means of national circulation, at the expense of the company;
- seizure of the product and all goods, effects, objects, documents and instruments involved in the commission of the crime; and
- whenever an offence involves investment of resources by the legal entity of an amount higher than the income it generates, imposition of a further penalty of an amount equivalent to the investment, to be paid to the Treasury.

Some of the penalties that were introduced for cases of criminal liability of companies have also been included as sanctions in civil enforcement cases, in particular a temporary ban on entering into contracts with state entities, which has been included as a sanction in cartel cases. The new Financial Market Commission, following this trend, has the facility to revoke the authorisation of existence of a stock corporation in certain cases.

iii Compliance programmes

As previously described, the undertaking of compliance programmes is encouraged by Law No. 20,393 (and is unique to it), for the purpose of not only being exempt from liability but also to mitigate it. The existence of these prevention models or programmes is a factor

---

9 To name one example, in antitrust matters, the maximum applicable monetary sanction was increased last year from 30,000 annual tax units (unidades tributarias anuales) (approximately 17,165,160,000 Chilean pesos) in cartel cases to 30 per cent of the sales of the offender during the period and in the line of business to which the infringement refers, or double the economic benefit obtained by the illegal conduct. If it is not possible to establish these amounts, the maximum fine can now be up to 60,000 annual tax units (approximately 33,819,840,000 Chilean pesos).
that may release the company from its liability. For these purposes, the law sets forth certain parameters that these compliance programmes should include. The minimum elements required by Law No. 20,393 are:

\[\text{a}\] the identification of the activities or processes of the company, whether habitual or sporadic, in whose context the risk of commission of the offences that can trigger the criminal liability of the legal person emerges or increases;

\[\text{b}\] the establishment of specific protocols, rules and procedures that allow persons involved in the above-mentioned activities or processes to execute their tasks in a manner that prevents the commission of the relevant offences;

\[\text{c}\] the identification of administrative and auditing procedures related to financial resources of the company that allow the entity to prevent their use to commit any of the offences to which the law refers; and

\[\text{d}\] the existence of internal administrative sanctions, and procedures for reporting or pursuing the pecuniary responsibility of any person who violates the prevention system.

Companies may have their compliance programmes certified by accreditation entities registered before the Superintendency of Securities and Insurance.

Furthermore, if a company did not have a compliance programme in place at the time a criminal investigation against it started and it sets up efficient compliance mechanisms before the beginning of a trial to prevent further commission of some of the offences that led to the liability, that action may constitute a mitigating circumstance.

**iv. Prosecution of individuals**

Liability may be attributed (1) solely to natural persons, (2) solely to legal entities or (3) jointly to both; it is not necessary to prosecute the natural person directly involved in the commission of the offence to impose liability on the company. There is no special provision dealing with the possibility of the same lawyers representing the legal entities and the natural persons involved, and joint representation is common, except when the defence strategies are incompatible; the Bar Code of Ethics and the Criminal Procedure Code are closely followed.

To establish criminal liability of companies, the criteria previously described must be met. On this basis, decisions made concerning the defence of individuals and the same company may present complex problems to be resolved according to the strategic planning of the company and the interests of the individuals.

Should there be a divergence of interests, defences will be incompatible; the Criminal Procedure Code even confers authority on the court to determine this incompatibility and request assignment of new defence counsel. However, there is nothing preventing defences being coordinated or planned in the case of common interests or even preventing the company from paying the lawyers’ fees of the individuals being prosecuted.

It is clear that there are circumstances in which this analysis may be hindered. For example, if the company cooperates with an investigation undertaken by the relevant state agencies, in cases where one member of the company is being investigated, the company can neither oblige them nor force them to cooperate. Conversely, taking measures against whistle-blowers may be inconvenient for the company and not recommended in terms of eventual liability arising from labour laws, for example. It may also damage the defence strategy of the company itself.
IV INTERNATIONAL

i Extraterritorial jurisdiction

The rules on criminal liability of corporate entities – the vast majority of the criminal laws in Chile – are governed by the principle of territoriality (i.e., they are only applicable when the offences were committed in Chile). This principle has certain exceptions in Article 6 of the Organic Code of Courts, but all refer to individuals. However, since Chilean courts have jurisdiction in cases of bribery of a foreign public official committed abroad by a Chilean national or a foreign national with residence in Chile, if the bribe was committed in the interest of or for the benefit of the legal entity, criminal liability of the latter may also be pursued in Chile.

In 2016, a specific provision was introduced in connection with extraterritorial jurisdiction of Chilean courts in antitrust criminal cases (cartels), provided the collusion has an impact in Chilean markets.

To date there are no relevant precedents in which an act committed abroad has led to enforcement by Chilean agencies in connection with that act. In certain cases, when Chilean companies have been subject to investigations abroad, this has led to agencies in Chile to investigate whether the conduct has been also committed in Chile.

ii International cooperation

The Attorney General and the courts, through direct requests as well as international pleas, are in permanent contact with foreign agencies for the purposes of international cooperation. This action is enshrined through various direct cooperation agreements among prosecuting entities as well as international treaties. An example hereof is the cooperation among Chilean and Brazilian public prosecutors in connection with potential ramifications of the Lava Jato case in Chile. Cooperation is not only common in criminal prosecution but also between some state agencies, such as the Financial Market Commission in securities enforcement procedures and the National Economic Prosecutor regarding antitrust regulations.

Chile has entered into many bilateral and multilateral extradition treaties. Extradition procedures regularly apply in Chile and are carried out with the intervention of the Supreme Court.

For an extradition request to be granted, in general, the crime needs to be punishable in both countries, and the prosecution in the requesting country must relate only to the crime for which extradition is granted. The sanction for the crimes for which extradition is requested must exceed one year.

iii Local law considerations

When a crime leads to the application of diverse rules of prosecution, practice says that the domestic authorities must apply domestic law; for those in charge of the prosecution, domestic law is mandatory, it being understood that international treaties signed by the country make them part of the domestic legislation. These treaties have been approved by the domestic legislators provided that said treaties comply with the Constitution. Therefore, special regulations in Chile regarding privilege, banking secrecy, admissible evidence, etc. will govern the matter in Chile.
V YEAR IN REVIEW

As has been the case since mid 2014, when the *Penta* case came to light, the most prominent investigations during the past 12 months have been in cases related to irregular funding of political campaigns, which have led to several tax fraud investigations and, in certain cases, to the prosecution of alleged bribery. Many companies (some of them listed) and some of their high-level officers are involved in these investigations as they contributed to political campaigns by means other than those explicitly contemplated by law, in what seems to have been an extended practice in Chile in the past. Last year, the Public Prosecutor’s Office closed the investigation on the *Penta* case and filed a formal accusation against 40 persons, including some companies. However, the investigation has been reopened several times. Recently the Public Prosecutor’s Office reached an agreement with some of the principal defendants for the application of an abbreviated proceeding, in which the accused accept the facts of the Public Prosecutor’s Office’s accusation in exchange for not having to risk a penalty of more than five years’ imprisonment, which is the limit for applying for probation. This agreement is expected to be brought before court shortly and is expected to be followed by agreements with the rest of the defendants.

On the other hand, in the *SQM* case, another prominent investigation regarding irregular funding of political campaigns, the Public Prosecutor’s Office entered into a deferred prosecution agreement with the legal entity (SQM), which was under investigation for its responsibility in the alleged bribery made by the entity administration. Under the agreement, which was approved by the court, SQM will have to pay approximately US$4 million to the state and charity organisations. It will also have to adopt anti-corruption measures, including the undertaking of a prevention programme. A similar agreement took place previously between SQM and the Securities and Exchange Commission and the United States Justice Department, having paid SQM fines of more than US$30 million to both entities. Finally, regarding the individual defendants, the public prosecutor in the *SQM* case is expected to close the investigation and file a formal accusation against a number of persons later this year.

Also on the criminal front, the last few years have been marked by the proliferation of Ponzi scheme fraud cases, in which investment companies attracted investors with the promise of high guaranteed returns that they paid mostly from money raised from new investors. All these cases imply a loss for over 10,000 affected investors in an aggregate amount of allegedly more than US$300 million. The investigations of these frauds are continuing.

In the context of cartel investigations, a case in 2017 involving price fixing in the tissue paper industry went to trial before the competition courts, where the National Economic Prosecutor requested a fine of 20,000 annual tax units\(^{10}\) in respect of one of the involved companies, and the exemption from a fine of the company that made use of the leniency mechanism set forth in antitrust law. The company that applied for leniency agreed on the consumer protection front to pay compensation in an aggregate amount of 97,647 million pesos, to be distributed among every Chilean adult residing in Chile. This amount is equivalent to 78 per cent of the profits obtained by the company during the 10 years during which the cartel was in place. In December 2017, the Court for the Defence of Free Competition upheld the National Economic Prosecutor’s request, imposing a fine of 20,000 annual tax

\(^{10}\) Approximately 11,412,586,800 pesos.
units\textsuperscript{11} to one of the companies involved, and exempting the company that made use of the leniency mechanism. This is the fifth case in which a company applied for leniency in the context of antitrust investigations since the mechanism was introduced in 2009, proving that it has been an effective measure to expose cartels in Chile.

A new law enacted in 2016 deems collusion to be not only an administrative infringement but also a crime (Law No. 20,945 – see Section II.i). The law extends the benefits of leniency agreements to the potential criminal proceeding, granting a reduction in the applicable penalties. On the other hand, the criminal proceeding may only be initiated by a complaint filed by the National Economic Prosecutor once the existence of the cartel has been established by a final judgment of the competition courts. The National Economic Prosecutor is obliged to file the criminal action in cases where the free competition of markets is seriously affected by the illegal conduct.

VI CONCLUSIONS AND OUTLOOK

In recent years, and particularly the past decade, Chile’s legislation on enforcement of penalties against illegal conduct has been undergoing a continuous and profound process of reformation. This has included the incorporation of new crimes and the updating of existing felonies, adjusting Chile’s legislation to international best practices, particularly in the area of anti-corruption and money laundering. We can highlight, for example, the inclusion of a crime of bribery related to foreign public officials and the approval of the law that establishes the criminal responsibility of legal entities.

In addition, various enforcement agencies have been restructured and in general given more investigative powers; for example, the restructuring of the Superintendency of Securities and Insurance, which changed its legal form completely from a superintendency managed by one person to a collective commission, the Financial Market Commission, and strengthened its investigative powers.

All these changes and the number and size of cases that have emerged in the past few years have had an important impact and are changing Chile’s legal culture from a reactive to a proactive approach.

In particular, the improvement in the description of offences sanctioned under the Criminal Code and the inclusion of new prohibitions, following the entry into force of the Law on Criminal Liability of Legal Entities, has had an important effect on the perception of the relevance of compliance in companies, particularly in entities engaged in activities where there is a potential risk of these kinds of conduct.

However, owing to the relative newness of the law, there have not been many cases to date in which anti-corruption laws have been enforced against legal entities. There are some that have ended in abbreviated proceedings or deferred prosecution agreements, and, so far, only one case has faced real trial, in which the legal entity was absolved because the individual who committed bribery was the only representative of the company; the court therefore estimated that sanctioning both the individual and the legal entity affects the double-jeopardy principle. In that same way, compliance programmes implemented by companies, which may exempt companies from liability if they are adequate, have not yet been tested by public

\textsuperscript{11} Id.
prosecutors or the courts. When more cases arise, it will be interesting to follow the outcome of the trials and the capability of the public prosecutors to verify the suitability of compliance programmes, as they have no experience in such matters as yet.

Furthermore, new significant legal changes that will affect the enforcement of corporate conduct are expected to be approved soon and enter into force in the next few months. For example, a Bill presented to Congress last year aims, among other things, to include the banking supervision authority in the newly created Financial Markets Commission. By this means the banking, insurance and securities market supervision will fall under the scope of a sole supervisory body.

On June 2015, as a reaction to some high-profile alleged corruption cases (particularly those involving irregular funding of political campaigns), a Bill was presented to Congress for discussion, proposing important amendments to anti-corruption regulation, including the increase of penalties for bribery and other corruption crimes, amendments to provisions related to bribery of foreign governmental officials, following recent recommendations issued by the OECD, and the regulation and punishment of commercial bribery, which so far is not considered a crime under Chilean law. The Bill is still under discussion in Congress.
Chapter 9

DENMARK

Jacob Møller Dirksen

I  INTRODUCTION

A number of agencies are empowered to investigate corporate conduct. Among these are the Danish Public Prosecution Authority (encompassing the State Prosecutor for Serious Economic and International Crime and the Danish Money Laundering Secretariat), the Danish Financial Supervisory Authority, the Danish Data Protection Agency and the Danish Competition and Consumer Authority.

The Public Prosecution Authority deals exclusively with cases concerning criminal investigation and prosecution. Its primary responsibility is to decide on whether to pursue criminal prosecution and to appear before the courts in criminal cases.

The State Prosecutor for Serious Economic and International Crime (SEIC) is a special unit within the Public Prosecution Authority that investigates and prosecutes cases concerning particular economic crimes, that is, where the economic crime is of significance, part of organised criminal activity, based on extraordinary business measures or is otherwise of a qualifying character. Examples of cases dealt with by the SEIC are bribery and corruption and other closely related offences, competition law violations and money laundering. The SEIC is also responsible for handling international criminal cases, such as genocide, crimes against humanity and other serious offences in which the criminal act has been perpetrated abroad and the investigation and prosecution presupposes cooperation with foreign institutions and authorities. The SEIC has very broad investigative powers and has a special position in Denmark owing to its specialised powers.

The Money Laundering Secretariat is the Danish financial intelligence unit (FIU) and sits within the SEIC. The main responsibilities of the Secretariat are receiving, analysing or communicating notifications to businesses when there is a suspicion of money laundering. Certain businesses, such as financial institutions, are subject to a number of inspection and reporting duties under the provisions of the Money Laundering Act in order to prevent money laundering. The Secretariat also receives notification of money laundering from public authorities. Upon receipt of a notification of potential money laundering, the Secretariat determines whether to request that the police initiate further investigations to lodge an indictment; the police decide whether to carry out any investigations. The Secretariat can, when needed, assist the police in obtaining information from Interpol or other countries’ FIUs. It also handles transit cases (i.e., where there are no personal or legal entity ties to Denmark) with no involvement by other authorities.

1 Jacob Møller Dirksen is a partner at Horten Law Firm.
The Financial Supervisory Authority (FSA) operates under the auspices of the Minister for Economic and Business Affairs and supervises financial businesses in Denmark. The primary task of the FSA is supervision of financial undertakings. It also supervises the securities markets and conducts regular inspections of the relevant financial institutions. The FSA can issue warnings, impose injunctions and, in severe cases, is empowered to revoke necessary business licences. If the FSA detects illegal activity, it will report the business to the SEIC for further investigation.

The Danish Data Protection Agency (DDPA) monitors businesses in order to ensure compliance with the Act on Processing of Personal Data. The DDPA can initiate its own investigations if the agency suspects a violation of the law. It also receives citizen complaints, and, after receiving these, can decide whether specific data-processing measures are in accordance with the regulations. The DDPA is empowered to inspect private businesses (and public authorities) to make sure that the processing of data is carried out in accordance with the Act on Processing of Personal Data.

The DDPA conducts inspections several times a year. If it discovers a violation of the Act on Processing of Personal Data, it is empowered to issue a ban on further data processing. In some cases, the DDPA will report the violation to the police, which then takes over the investigation.

The Danish Competition and Consumer Authority (DCCA) enforces the Danish Competition Act. It is an authority within the Ministry of Business and Growth of the Danish government. The DCCA handles the daily operations of the administration of the Competition Act on behalf of the Competition Council. Unlike most other enforcers in Europe and elsewhere, the DCCA cannot issue fines but must forward cases to the public prosecutor. In limited cases involving minor infringements, it is authorised to make administrative determinations, such as dawn raids. Investigations may be triggered in different ways, but typically by reports or complaints from competitors and consumers. The DCCA may also carry out investigations on its own initiative, if it suspects that a certain company has violated the Competition Act. The DCCA regularly carries out dawn raids in Denmark. Investigation and prosecution of criminal cases must be undertaken by the SEIC as the DCCA does not have authority to investigate or prosecute criminal cases before the courts.

The various authorities are empowered with different investigatory tools. The SEIC has very broad investigation powers, and those regarding dawn raids are much broader than the powers of the DCCA; the SEIC may seize documents during dawn raids, but the DCCA is only allowed to take copies of the information it wants.

Political agendas and domestic priorities have no impact on the prosecutorial functions. The authorities act independently and without any political influence.

A business under investigation has no obligation to cooperate with the authorities and taking an adversarial stance is both a realistic possibility and common.

Criminal investigations are handled exclusively by the authorities, that is to say, internal investigations by a business entity are not admissible in court. The authorities are obliged to remain neutral and objective in the course of their investigation and to share the information obtained through this investigation with their subject.

The Danish Criminal Code is the codification and the foundation of criminal law in Denmark. It is divided into a General Part of 97 sections and a Special Part of 208 sections. The main legal source of the rules of jurisdiction in Denmark in civil and commercial matters is the Danish Administration of Justice Act.
II CONDUCT

i Self-reporting

There is no general legal obligation to self-report. In determining whether to self-report, the seriousness of the offence and the leniency opportunities should be taken into account.

Cooperating with the authorities can benefit a company that self-reports. Cooperating may lead to a reduction in fines, and in some cases, the public authorities may even decide against commencing criminal charges.

Article 82 of the Criminal Code lists a number of mitigating circumstances for criminal conduct. These can lead to a reduction of the penalty upon conviction. The circumstances are primarily meant for individuals, but can also be relevant for a legal entity, for example, self-reporting or volunteering information on the illegal activities of third parties. It is at the discretion of the court to determine whether self-reporting or volunteering information about third parties should have an influence on the sentencing. Except in matters of cartel regulation, no written policies or guidelines are available as to when self-reporting may lead to benefits for businesses.

Under the Competition Act, a member of a cartel may apply for impunity or leniency. Businesses that participate in a cartel can be punished by fines in excess of 20 million Danish kroner, although if there are mitigating circumstances, the fine may be lower. Executives and board members can be individually fined (usually several hundred thousand kroner) or sentenced to imprisonment for up to six years in very severe cases. Application for impunity is available to members of a cartel under the Competition Act, Section 23a. Impunity may be granted by the SEIC if the cartel member (applicant) is the first to report the cartel to the authorities, the applicant provides information that the authorities were not previous privy to, or the information provides grounds for investigative measures (inspection, dawn raid or police reporting) or grounds for establishing a violation of the Competition Act. The applicant must cooperate with the authorities throughout the investigation, must have ceased any participation in the cartel at the time of application and may not have forced any other business to participate in the cartel. If the applicant is not the first member of the cartel to self-report, the applicant may obtain a reduced fine under certain circumstances; that is, the information provided by the applicant regarding the cartel must add significant value for the authorities relative to the information already available, the applicant must cooperate with the authorities throughout the investigation, the applicant must have ceased any participation in the cartel at the time of application and may not have forced any other business to participate in the cartel. The second applicant in the cartel may obtain a 50 per cent reduction of the fine, the third applicant a 30 per cent reduction and applicants thereafter a 20 per cent reduction. The prosecutor will inform the court of the applicants’ participation and fulfilment of the requirements for leniency. Applications will be treated with discretion, but no guarantees of confidentiality can be issued. In cases where the cartel involves other EU Member States, the authorities have an obligation to report the cartel to the EU Commission and provide information about the identity of the applicants for leniency. The DCCA is also obliged to publish information about judgments and fixed-penalty notices issued against cartel members.

ii Internal investigations

A business may conduct its own internal investigation at any time, but there are no legal requirements as to when and how the investigation must be conducted.
The extent of the internal investigation will vary and depend on the size of the business and the level of exposure. Witness interviews and scrutiny of documents are typical in internal investigations; these are typically conducted by law firms (external counsel). The external counsel will have no subpoena powers or otherwise, but must rely on the cooperation of the company and its employees, that is, it must rely on the company providing access to the relevant documents and granting interviews with relevant witnesses. A waiver of privilege would be expected as part of the company's cooperation. It is not unusual for the employees being interviewed to be assisted by independent counsel.

The investigations should be carried out in accordance with the Data Protection Law and Danish employment law. There is no legal obligation for a company to disclose the findings of an internal investigation to the authorities.

### Whistle-blowers

Whistle-blowers are a hot topic in Denmark. Increasingly whistle-blower systems have become commonly applied by Danish businesses, as the systems allow the employees a safe place to share their knowledge. Whistle-blower systems are often seen as part of an effective compliance programme as a way the employees can either report an illegal activity within the company or seek guidance regarding potential cases of non-compliance.

Companies that have a whistle-blower system in place must ensure that it complies with Danish data protection rules. With the new General Data Protection Regulation (GDPR) effected, companies must no longer notify the DDPA of whistle-blower systems.

The DDPA is of the opinion that reporting may only take place in cases of serious offences – of suspicion thereof – that can be of importance to the group or company as a whole, or that can be of significant importance to the life and well-being of individuals. This may include suspicion of serious economic crime, including bribery, fraud and forgery.

The DDPA has taken the view that reporting can take place to the degree required by the Sarbanes Oxley Act, namely for irregularities in the areas of accounting, internal auditing and suspicion of corruption and crime in the bank and finance sectors. Other examples deemed suitable by the DDPA include cases of environmental contamination, serious breaches of work safety and serious circumstances involving an employee, such as sexual abuse. However, less serious offences cannot be reported (e.g., cases of harassment, cooperative difficulties, incompetence, absence, violation of guidelines for, for example, attire, smoking or drinking, using email or the internet).

It is important to note that there is no statutory protection for whistle-blowers. The authorities have not implemented any specific incentive programmes for whistle-blowers to come forward.

Depending on the specific circumstances, a business may take lawful action (e.g., terminate employment) against employees reporting suspicion of illegal activities if this is done in a disloyal manner, such as involving the media, or in a manner that violates confidentiality obligations. If the business has fired an employee for acting as a whistle-blower and the termination is unlawful, the employee is entitled to damages but not to be reinstated within the business.

Only a few Danish cases have dealt specifically with employees reporting illegal activities. In the 2005 Grevil case (reported in Ugeskrift for Retsvæsen 2006.65 Ø), Frank Grevil, a former army intelligence officer, leaked classified information regarding the threat
reports from Iraq originating from the Military Intelligence Service, FET, to a journalist from a Danish newspaper. Frank Grevil was dismissed, found guilty of disclosing confidential information and was sentenced to six months’ imprisonment.

III ENFORCEMENT

i Corporate liability

Corporate liability for legal entities is available under Danish law.

Criminal liability of a legal entity is conditional upon a transgression having been committed within the establishment of the legal entity by the fault of an individual connected to the legal person or at the fault of the legal entity itself.

A legal entity can be prosecuted in a similar way to a physical person if the legal basis is present; it must be stipulated specifically in the law that the company is subject to criminal punishment if an offence is committed by the legal entity.

The relevant set of rules is found in Chapter 5 of the Criminal Code, which states that companies and corporate bodies can be subject to criminal liability. Criminal liability must involve the commission of a criminal act or omission by one or more physical persons acting on behalf of the legal entity. It is not a requirement that the person in question is a member of management. The company can be liable for any intentional or negligent criminal act or omission by its employees, contractors and agents acting on its behalf if the act or omission is not abnormal in the context of its usual business, practices and procedures. Generally, it would not be advisable – nor is it normal practice – for the company and individuals to be represented by the same counsel, but it is normal practice for counsel to cooperate on a defence.

ii Penalties

A company may be punished only by a fine, whereas individuals may be imprisoned. Imprisonment can generally only be imposed on managerial staff, but under special circumstances subordinate employees can also be charged with the offence.

Plea bargains are not available under Danish law, but an individual or corporate entity can accept a fine based on a fixed-penalty notice from the prosecutor. The amount of the fine will be determined after a consideration of the gravity of the offence, the duration of the offence and the turnover of the company.

A company can also be subject to confiscation, which follows from Section 75 of the Criminal Code. Confiscation is a possible penalty if the company has gained proceeds from a criminal act, and if the Danish Public Prosecution Authority decides on prosecution.

The range of potential sanctions does not vary, regardless of which authority brings the action, but the level of fines may vary depending on the subject matter.

iii Compliance programmes

During the past few years, there have been significant developments in establishing and practising compliance programmes in Denmark.

There is no regulation on compliance programmes nor any sentencing guidelines that take compliance programmes into account.

Compliance programmes primarily ensure that a business complies with the law, but the existence of a compliance programme also has some advantages in cases of non-compliance regarding the penalties. The existence of a compliance programme can serve as an argument against criminal charges or as an argument of mitigation of the penalty, for example, as a
reduction of a corporate fine. However, this is only a possibility and is at the discretion of the prosecutor and the courts to assess whether a compliance programme should be a mitigating factor. Generally, it will not be a mitigating factor if senior management has been involved in the offence.

iv Prosecution of individuals
Under Danish law, an employer has a right to decide whether an employee's contract should be terminated. However, the exercise of this right has been limited by statutes and by collective agreements, prescribing that a termination should be based on a fair reasoning. In this context, a fair reasoning means that the termination should either be reasonable according to the conditions of the company or the behaviour or conditions of the employee. Criminal charges against an individual would normally be sufficient for a lawful termination.

The company may coordinate with the employee's individual counsel and it may be advisable for the company to retain the employee until after the criminal investigation has been finalised or even until after a judgment has been rendered. The company will be able to cooperate with the investigation and retain the employee. The company can advance or pay the legal fees of the employee's counsel, but this may create complex tax issues.

IV INTERNATIONAL

i Extraterritorial jurisdiction
Danish law applies when a criminal offence is committed outside Denmark if the suspect is either a Danish citizen or a permanent resident in Denmark, and if the offence is recognised as a criminal act in Denmark.

The Criminal Code specifies that Danish courts have jurisdiction in offences committed outside Denmark, if the offence is committed by either a Danish citizen or a permanent resident in Denmark, or if the citizen who committed the offence becomes a Danish citizen or a permanent resident after having committed the offence.

ii International cooperation
The Nordic countries – Denmark, Finland, Iceland, Norway and Sweden – cooperate closely regarding criminal investigations and crime prevention. On the basis of cross-national influences between historically interrelated and culturally (relatively) similar countries, this cooperation is successful.

Denmark has ratified a number of conventions to address criminal activity. Among these are the Schengen Agreement 1995, the European Conventions on Mutual Assistance in Criminal Matters 1959 and 2000, and a further number of UN and EU conventions. Furthermore, Denmark is an active member of several international networks, including Europol, the OECD and Interpol.

Extradition is possible under the auspices of the European arrest warrant and pursuant to individually negotiated treaties with countries outside the European Union. Extradition is not common but it does occur.

iii Local law considerations
The Danish authorities are very reluctant to recognise investigatory measures that are foreign to Danish law. The authorities will recognise foreign criminal investigations that comply with Danish law and particularly if the Danish authorities are involved in the investigation.
V YEAR IN REVIEW

The GDPR is a new EU regulation intended to strengthen and unify data protection. It entered into force on 5 May 2016, and Denmark and other EU Member States transposed it into their national laws with effect from 25 May 2018. It replaces the old data protection Directive of 1995.

The primary objectives of the GDPR are to give citizens and residents control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the European Union. One of the more extensive provisions of the new regulation is that businesses must appoint a data protection officer to be in charge of supervising and ensuring an organisation’s compliance with the GDPR.

In general, the new regulation aggravates the standards of administration of personal data and imposes a considerably higher level of fines; a serious violation of the regulation can lead to a penalty as high as €20 million or 4 per cent of global turnover.

Despite the increased effort, the Financial Action Task Force (FATF) does not consider Denmark’s effort in combating money laundering as sufficient. In its report of August 2017, the FATF criticises Denmark for not having a national strategy to combat money laundering and terrorist financing, and points out that Denmark needs to do more to properly assess and understand the risks it is exposed to. The report also recommends that Denmark enacts an independent and modern money laundering offence that criminalises self-laundering. Businesses may therefore expect further measures by the authorities regarding money laundering. In June 2017, a Bill entered into force to implement the Fourth EU Anti-Money Laundering Directive,2 and thereby implement certain changes to the current regulation on money laundering. The Bill seeks to implement the recommendations made by the FATF. Among other things, the Bill extends the scope of application, amends certain definitions, obligates a business to continuously assess its risk for being involved in money laundering, and entails more thorough customer assessment procedures and changes to the notification procedures. Since the Bill was implemented, the SEIC has received more tip-offs regarding money laundering than ever before.

In January 2017, the Danish High Court imposed a record-breaking fine for money laundering (Eastern High Court judgment of 26 January 2017 in Case No. S-317-16). The fine was 111 million kroner for the laundering of 223 million kroner through an exchange bureau. Two individuals (managers) were each sentenced to six years in prison. The judgment put an end to the activities of both the managers and the exchange bureau. The case is the first of its kind in Denmark, but it coincides with the fact that the authorities have increased their efforts to combat money laundering.

In March 2017, the Danish High Court imposed a record-breaking fine of 13 million kroner for market abuse (Eastern High Court judgment of 23 March 2017 in Case No. S-2410-15). The former chief executive officer (CEO) and chairman of the board of the company were both sentenced to 18 months’ imprisonment and their proceeds from divestments of shares in the company (800,000 and 9 million kroner respectively) were confiscated. The case concerned the legality of the purchase of treasury shares between November 2007 and October 2008 in the amount of approximately 100 million kroner. The

---

company’s traders purchased the shares at the stock exchange with the purpose of using them as payment in connection with the fulfilment of agreements with third parties and to fulfil options programmes with senior staff, including the CEO and the chairman of the board.

The High Court found that the company by its actions had ensured that the stock price was artificially high compared to the market value and that the activities gave the market wrongful or misleading signals regarding the stock price. The company’s traders bought so many shares that the company obtained a dominant position in the market or, through its traders, the company placed orders, for example in closed auctions at the best price, which was significantly above the latest updated price at the stock exchange.

The case is significant in view of the sanctions imposed and because the prosecutor in previous years has failed to obtain convictions in cases involving market abuse.

In June 2017, the Danish High Court found that the founder and board member of a collapsed bank was not guilty of committing fraud in relation to him acting for private interests in commercial matters. The case is significant as the High Court changed the judgment of the district court, which had sentenced the founder and board member to 30 months in prison. The case concerned an issue of options at a price that was too high by 5 million kroner, which led to an increased risk for the debt holders of the company. The High Court, unlike the district court, did not find that the contract behind the share purchase was unusual in a commercial context.

The case is one of several concerning collapsed banks in recent years.

VI CONCLUSIONS AND OUTLOOK

Implementation of the GDPR has received significant attention and this trend is likely to continue.

The Bill implementing the Fourth EU Anti-Money Laundering Directive will also continue to receive attention, as businesses will continuously have to implement new procedures on the assessment of their risk in participating in money laundering.

Generally, we expect that cross-border investigations will be prioritised by the authorities and that the necessary resources will be allocated to the authorities to deal with the complex issues and to cooperate with foreign authorities.
I INTRODUCTION

The investigation and prosecution of corporate offences, historically, has been low on the list of priorities for the United Kingdom. In more recent years, however, sustained international criticism, the financial crisis and increasing public anger have prompted increased efforts by a range of government bodies to combat corporate offending. Recent data leaks, including the Panama and Paradise Papers and the controversy focusing on Unaoil, have added to the upward trajectory.

Several bodies are responsible for investigating and prosecuting corporate offending in England and Wales. These include the Serious Fraud Office (SFO), the Competition and Markets Authority (CMA), the Financial Conduct Authority (FCA), Her Majesty’s Revenue and Customs (HMRC) and the Office of Financial Sanctions Implementation (OFSI). While there is some overlap in the offences each of these bodies can investigate and prosecute, their remits are largely separate. In addition, the overlaps that do exist have been addressed by memoranda of understanding that assign primacy in the vast majority of investigations and prosecutions (although concurrent investigations occasionally do occur).

Each of the aforementioned bodies has a wide range of powers. Typically, they include the execution of dawn raids (whether alone or with the assistance of partner law enforcement agencies, such as the police or the National Crime Agency (NCA)) and the compulsory production of documents and information. Non-compliance with lawful production orders constitutes a criminal offence in the United Kingdom.

Importantly, the serving of compulsory production notices tends to override any duties of confidence a recipient otherwise owes to a third party (except with respect to legal professional privilege, which can, unless waived, operate to prevent disclosure – see Section IV.iii). Financial institutions and professional advisers must therefore comply with such notices, absent professional privilege, without fear of being held liable to their clients for breach of confidence.

The SFO is responsible for investigating and prosecuting the most serious cases of fraud and other related economic crimes in the United Kingdom. A large part of its remit involves the investigation and prosecution of bribery and corruption offences as well as certain financial and competition law offences. The SFO’s powers of investigation are derived from Section 2 of the Criminal Justice Act 1987 (CJA87), which permits the SFO to require persons to answer questions and produce documents.

---

1 John Rupp is a partner, Alex Melia is an international counsel and Peter Ibrahim and Andris Ivanovs are associates at Steptoe & Johnson UK LLP.
The SFO has the power to conduct dawn raids (with the practical assistance of the police and the NCA) and conducted several high-profile dawn raids in 2015 and 2016, including on the premises of Soma Oil and Gas in July 2015 and Unaoil in March 2016.

Having previously suffered a high-profile defeat in a dawn raid judicial review claim brought by the Tchenguiz brothers,\(^2\) the SFO more recently secured a significant victory when a judicial review claim brought by Unaoil challenging a letter of request preceding a dawn raid by the Monégasque authorities was rejected by the Administrative Court in March 2017.\(^3\) The Unaoil decision followed the rejection of a judicial review claim brought by Soma in August 2016.\(^4\) Although Soma’s judicial review claim was unsuccessful, the company did benefit from the judicial review process by obtaining a letter from the SFO stating that its investigation had not produced sufficient evidence to support bribery allegations. Unaoil’s setback does not appear to have discouraged companies wishing to challenge the SFO’s investigatory methods. The SFO opened an investigation into the UK subsidiaries of KBR, Inc in 2017 and the US company is now challenging the SFO’s power to compel production of documents located overseas, pursuant to Section 2 of the CJA87.

Dawn raids, too, have been used historically by the UK competition authorities. Since April 2014, the CMA has taken over the competition functions of the now defunct Office of Fair Trading (OFT) and the Competition Commission. The CMA is now the main competition regulator in the United Kingdom, being responsible for ensuring compliance with the Competition Act 1998 (CA98) and Articles 101 and 102 of the Treaty on the Functioning of the European Union.

In carrying out its functions, the CMA has wide-ranging powers derived from the CA98 to investigate suspected infringements of competition law. These include the power to request information, whether in the form of documents or answering questions, and to conduct various on-site investigations, including dawn raids, examining and making copies of company books and records and requiring computerised information to be produced in a form that is readable.

Since April 2015, the FCA has had concurrent competition law powers for the financial services sector pursuant to which it may, \textit{inter alia}, prosecute competition law infringements, conduct market studies and refer markets to the CMA for in-depth investigation. The FCA’s main remit, however, is regulating the financial services sector and maintaining the integrity of the UK financial markets.

\(^2\) \textit{Tchenguiz v. Serious Fraud Office} [2012] EWHC 2254 (Admin) dealt with the execution of a search warrant on the business premises of prominent UK businessmen Robert and Vincent Tchenguiz for documents pertaining to the collapse of the Icelandic bank Kaupthing. The High Court held in the foregoing case that the Serious Fraud Office (SFO) search had been unlawful because the SFO had obtained the underlying warrant through misrepresentation and that it had failed to disclose salient facts to the judge who had issued the warrant.

\(^3\) \textit{Unaenergy Group Holding Pte Ltd & Ors, R (on the Application of) v. The Director of the Serious Fraud Office} [2017] EWHC 600 (Admin). The High Court expressed reluctance in this case to permit challenges to the conduct of enforcement agencies, such as the SFO, acting in good faith to investigate serious criminality.

\(^4\) \textit{Soma Oil And Gas Ltd, R (on the Application of) v. Director of the Serious Fraud Office} [2016] EWHC 2471 (Admin).
A wide range of investigatory powers has been conferred upon the FCA by Section 168(2) of the Financial Services and Markets Act 2000 (FSMA). Investigations of this type typically relate to allegations of insider dealing, market abuse, making misleading statements, giving misleading impressions or violating the general prohibition appearing in Section 19 of the FSMA. Relevant powers include the power to interview any person (whether the subject of the investigation or not), compel the production of documents and information and compel any person to give such assistance as he or she is ‘reasonably able to give’.

HMRC is responsible for investigating tax and revenue-related offences in England and Wales. In doing so, it has a wide range of civil and criminal investigatory powers. Its civil powers derive from the Finance Act 2008 and include the power to obtain information and documents under compulsion and to inspect premises. HMRC’s criminal powers are derived from a range of statutes, the main one being the Police and Criminal Evidence Act 1984 (PACE). The PACE confers a broad range of investigative powers on HMRC, including search and seizure and compulsory document production.

The OFSI is responsible for implementing the financial sanctions regime within the United Kingdom. The OFSI monitors compliance with the regime and is notified of any suspected violations. The OFSI has the power under the Policing and Crime Act 2017 (PCA) to impose monetary penalties for any breaches of the financial sanctions legislation. Under this new regime, a monetary penalty of up to £1 million can be imposed on a person if the OFSI is satisfied it is more likely than not that a particular person breached or failed to comply with the UK financial sanctions regime. If a breach or failure relates to particular funds or economic resources and it is possible to value them, the maximum fine the OFSI can impose is the greater of either £1 million or 50 per cent of the estimated value of the funds or resources. As such, when it is possible to put a value on the breach, the fine could be significantly in excess of £1 million.

The SFO, the CMA and the FCA are empowered to investigate and prosecute relevant offences falling within their remit. HMRC and the OFSI, by contrast, are only responsible for investigation. The prosecution of tax and financial sanctions offences has been assigned to the Crown Prosecution Service (CPS). The decision to prosecute is required to be made in accordance with the Full Code Test in the Code for Crown Prosecutors in relation to criminal offences and applicable codes of practice or guidance otherwise.

II CONDUCT

i Self-reporting

Against a backdrop of ever-increasing regulation and enforcement, self-reporting is an issue many corporates have to grapple with at some stage. The starting point for the majority will be the same: while there is, in general, no legal obligation to self-report in the United Kingdom, self-reporting may or may not – depending upon a variety of factors and circumstances – be advantageous.

---

5 Section 19 of the Financial Services and Markets Act 2000 makes it a criminal offence to carry out any regulated activities in the United Kingdom without prior authorisation from the Financial Conduct Authority (FCA).

The most well-developed self-reporting regime is operated by the CMA in relation to cartels, which provides for three types of immunity or leniency for corporates from the imposition of financial penalties. Whether full immunity is granted will depend largely upon the timing of the self-report. Greater credit is given the earlier the self-report is made. Broadly, the first to report, provided the self-report is made before the CMA has begun its own investigation, will qualify for leniency (subject to the satisfaction of additional criteria).

A discretionary sliding scale of leniency is offered to those who come forward after an investigation has begun or when the particular corporate is not the first to do so. The highest and broadest type of leniency, Type A, can offer full corporate immunity from fines and immunity from criminal prosecution for all current and former directors, officers and employees who cooperate with the CMA. Timely self-reporting, therefore, can be crucial in the context of competition infringements.

A less generous but nonetheless significant self-reporting regime is operated by the SFO. While the SFO’s guidance on corporate prosecutions has made clear for some time that a self-report may be taken into account as a public interest factor tending against prosecution, only recently – with the advent of Bribery Act 2010 (BA) offences, the availability of deferred prosecution agreements (DPAs) and an increasingly aggressive approach by the SFO – has this guidance actually begun to prompt some self-reporting.

Standard Bank was the first company to enter into a DPA, having self-reported possible misconduct before having begun an internal investigation. In a contrasting case, the Sweett Group self-reported potential misconduct only after allegations of misconduct had appeared in the press. The difference in outcome is striking: the Sweett Group was convicted of a criminal offence while Standard Bank paid a civil fine (although it should be noted that a number of additional factors are likely to have contributed to the differential outcomes of the Standard Bank and Sweett Group matters).

The approach taken by Standard Bank was praised by the court. Further, in presenting the proposed DPA to the court, the SFO stated that Standard Bank’s early self-report had been a major factor causing the SFO to seek to resolve its investigation of Standard Bank by means of a DPA. Meanwhile, the Sweett Group does not appear to have obtained any meaningful credit from the SFO or the court for what both apparently concluded had been an unjustifiably belated self-report.

A company anonymised as XYZ Limited was the second company to enter into a DPA, in July 2016. Like Standard Bank, XYZ self-reported following concerns that came to light during the implementation of a new global compliance programme. In approving the proposed DPA, the court placed considerable weight on the timing of XYZ’s self-report and its ‘genuinely proactive’ approach to the wrongdoing that was discovered. The court also awarded a 50 per cent reduction in the fine levied against the company in settlement of the case in light of the company’s early self-report.

---

7 Although the Competition and Markets Authority (CMA) does carry out both civil and criminal investigations, only individuals may be prosecuted for the criminal cartel offence. Corporates are only liable to financial penalties.


The third corporate DPA represented a departure from the principles established in the Standard Bank and XYZ cases. In January 2017, Rolls-Royce became the first company to secure a DPA without having first self-reported to the SFO.\(^\text{12}\) As with XYZ, the court awarded Rolls-Royce a 50 per cent reduction in the fine levied in settlement of the case. While the court stated in its judgment that self-reporting continues to be ‘highly relevant’ when determining whether to approve a DPA, the court nonetheless was persuaded that the ‘extraordinary cooperation’ of Rolls-Royce rendered a DPA appropriate. Among other things, Rolls-Royce provided the SFO with access to memoranda of internal interviews in respect of which privilege could have been claimed, and deferred internal interviews to allow the SFO to question individuals before they were interviewed by company representatives.

It is unclear whether Rolls-Royce’s ability to secure a DPA without first having self-reported will curb companies’ enthusiasm for self-reporting in the future. The former head of the SFO, David Green QC, who retired in April 2018, had always advocated the benefits of self-reporting, repeating Sir Brian Leveson’s proclamation from the XYZ DPA that ‘incentivising self-reporting is a core purpose of DPAs’.\(^\text{13}\) Alun Milford, the General Counsel of the SFO, has pointed out that because it did not self-report its misconduct, Rolls-Royce started at a disadvantage. This was outweighed by its subsequent cooperation and provision of relevant information, which was ‘far more extensive and of a different order’ to what the SFO would have learned without the company’s cooperation.\(^\text{14}\) Nevertheless, it remains to be seen what approach companies will take in the future now that a failure to self-report has not been deemed in itself to be an outright bar to securing a DPA.

The FCA has had a longer history than the SFO of taking significant and consistent enforcement action against the firms it regulates. Self-reporting by FCA-regulated firms is far more routine for the FCA than the SFO – indeed, it is largely compulsory. Pursuant to the FCA’s high-level principles for business, regulated firms are required to deal with the FCA in an open and cooperative way, disclosing anything relating to the firm and the firm’s corporate group of which the FCA reasonably would expect notice.\(^\text{15}\) Suspicion or evidence of wrongdoing by FCA-regulated firms falls within the scope of this requirement and thus should be – and generally is – reported to the FCA as a matter of course.

Since July 2015, the foregoing self-reporting obligations have been extended to competition law infringements.\(^\text{16}\) Consequently, FCA-regulated firms now are expected to self-report instances of significant infringements of competition law to the FCA. Self-reporting generally is regarded, as has been stressed in recent FCA pronouncements, to

---

12 [2017] Lloyd’s Rep FC 249.
be a bare minimum requirement by the FCA\textsuperscript{17} and enforcement action is typically taken if that requirement is breached. Recent enforcement actions reflecting this trend ended with Deutsche Bank AG being fined £227 million for misconduct in manipulating LIBOR and EURIBOR and the bank’s failure to deal with the FCA in an open and cooperative way\textsuperscript{18} and Sonali Bank (UK) Limited being fined £3.25 million for inadequate anti-money laundering controls and a similar failure to deal with the FCA openly and cooperatively\textsuperscript{19}.

The decision to self-report in the United Kingdom is often influenced or driven by the application of the UK money laundering regime. The Proceeds of Crime Act 2002 (POCA) includes several money laundering offences predicated on the commission of one or more criminal offences that have produced revenues in or resulted in revenues being remitted into the United Kingdom. Broadly, the only way liability for the POCA offences can be avoided is by reporting the underlying criminal conduct. That is especially so for those operating in the regulated sector – for the most part, financial institutions and professional advisers – who are subject to function-specific reporting obligations under the POCA.

\section*{Internal investigations}

Internal investigations have become increasingly common due largely to the increase in UK enforcement action and the severity of penalties that increasingly are being imposed. While the authorities do not necessarily require corporates to carry out internal investigations when they suspect wrongdoing, they typically expect to see that some action has been taken when evidence of possible misconduct is discovered or reports of possible misconduct are received. The type of action that is expected varies, however, between and among the pertinent authorities.

Internal investigations may be conducted by either internal or external counsel. Internal counsel typically takes the lead in conducting internal investigations when the misconduct at issue is of a minor or routine nature. In cases involving more serious misconduct, and particularly when there is a tangible possibility of enforcement action, it is more typical for external counsel to take the lead.

The SFO has made it clear that the primary responsibility for investigating possible misconduct within the SFO’s remit falls squarely upon the SFO.\textsuperscript{20} That said, SFO officials have said that they understand that ‘up to a point’ corporates will need to do some work to investigate possible misconduct, if only to determine preliminarily whether the evidence of misconduct that has been discovered or the report of misconduct that has been received warrants the SFO’s attention.

\begin{flushright}
\end{flushright}
At the same time, SFO officials have said repeatedly that they will not tolerate internal investigations that ‘trample over the crime scene’ and expect corporates to cooperate with the SFO’s investigation rather than duplicating it. Further, SFO officials stress that they will not accept self-reports at face value, no matter how comprehensive or seemingly objective the reports appear to be, being committed to conducting their own investigation to establish the pertinent facts.21

The SFO’s begrudging tolerance for internal investigations is in stark contrast with the encouragement that long has emanated from officials at the US Department of Justice (DOJ) and Securities and Exchange Commission (SEC). Given the SFO’s rather paltry budget, at least when compared with the resources that have been given to the DOJ and the SEC, the SFO’s attitude toward internal investigations is surprising.

In addition, it is not at all clear how a corporate-funded investigation would ‘trample over the crime scene’, particularly when such investigations are geared toward collecting and preserving potentially pertinent electronic and other evidence that may be lost by the mere passage of time or pursuant to the company’s long-standing document retention programme. Further, the SFO has not explained how its approach to internal investigations can be squared with a company’s duty, when suspecting past misconduct, to move promptly to avoid future misconduct – a responsibility that can be difficult to meet if the corporate is deprived of the ability to conduct a prompt internal investigation.

The SFO’s approach to internal investigations is mirrored in important respects by the FCA.22 While encouraging internal investigations in some contexts, the FCA has discouraged them when the suspicion that has arisen relates to market abuse or other criminal conduct. In those circumstances, the FCA expects firms not to carry out their own investigation, purportedly because of the risk of the FCA’s investigation being compromised or potential suspects being alerted. Importantly, the FCA – like the SFO – expects to be involved from an early stage to discuss the nature and scope of any internal investigation the particular company has proposed to undertake or commission.

Both the FCA and SFO expect corporates to provide them with the fruits of any internal investigation they have undertaken or commissioned and the underlying supporting materials. Although privileged material is said to be protected from mandatory production, the FCA and SFO often have demanded production of – at the very least – the factual narrative in any internal investigation report that has been prepared. In one recent case, a corporate reportedly negotiated a compromise agreement with the SFO, agreeing to provide an oral summary of the internal investigation report as well as underlying documents rather than the report itself. In other cases, corporates have chosen to provide the FCA and SFO with the full internal investigation report, seeking thereby to earn maximum cooperation credit.

Many have suggested, with good reason, that the decision of the High Court in Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Ltd23 will operate as a major deterrent to internal investigations in the United Kingdom if the High Court’s decision in the ENRC case is upheld by the Court of Appeal. In this case, discussed in more detail below, the High Court ordered ENRC to hand over various documents to the SFO, rejecting

22 FCA Handbook, EG 3.11.
a claim of litigation privilege in respect of most of the pertinent materials. The High Court’s
decision was sharply criticised by The Law Society, the independent professional body for
solicitors in England and Wales.24

Internal investigations tend to be conducted routinely in a competition law context,
typically to support leniency applications. The relatively low evidential threshold for such
applications, coupled with the significant advantages of an early application, usually result in
a more detailed internal investigation being carried out post-application. Both pre-application
and post-application internal investigations must be carried out with extreme caution,
however, because of the risk of ‘tipping off’ other participants in the suspected cartel activity.
The CMA has issued guidance on how that should be managed.25

Importantly, while the CMA does not require a waiver of legal privilege as a requirement
of leniency or otherwise, it does require corporates to keep a detailed note of all actions
undertaken as part of any internal investigation they have conducted or commissioned,
including recording the identities of any witnesses who were interviewed, the nature of the
questions that were asked of them and their respective responses. The note is required to be
retained until the conclusion of any proceedings the CMA initiates. Any refusal or inability to
do so may be viewed by the CMA as an application not meeting the conditions for leniency.

iii Whistle-blowers
Whistle-blowers are afforded a number of workplace and non-workplace protections in
England and Wales. Workplace protections derive from the Public Interest Disclosure Act
1998 (PIDA), which protects qualifying disclosures made to, inter alia, employers and
‘prescribed persons’, including the CMA, the SFO, the FCA and HMRC.

To qualify for protection, the disclosure must relate to a failure such as the commission
of a criminal offence or breach of a legal obligation. The disclosure also must be motivated
by a reasonable belief on the part of the whistle-blower that the failure occurred and that its
disclosure is in the public interest.

If the disclosure satisfies the PIDA criteria, it will be protected and employees dismissed
unfairly or suffering detriment as a result of their disclosure may seek potentially unlimited
compensation from their employer. Companies are expected to have procedures for dealing
with whistle-blowing, especially when regulated by the FCA.26 As a minimum, a company
will be expected to consider whether any further steps are required as a result of any disclosure,
such as whether further investigation or the implementation of remedial action is needed.

Non-workplace protection is given to witnesses and victims through the Code of
Practice for Victims of Crime and the Witness Charter, which most prosecuting authorities,
including the SFO and the FCA, are legally bound to apply. These provide broad protection

24 Max Walters, ‘Erosion of Privilege Lambasted by Society’ (The Law Society Gazette, 15 May 2017),
11 May 2018.
25 See July 2013 Office of Fair Trading (OFT) guidance for leniency and no-action in cartel cases, adopted by
the CMA at OFT, ‘Applications for leniency and no-action in cartel cases’ (London, July 2013, www.gov.uk/
26 The FCA has rules in relation to whistle-blowing requiring certain regulated firms to implement procedures
for handling whistle-blowing disclosures as well as a senior manager as their whistle-blowing champion.
to disclosures and the treatment of victims and witnesses. Importantly, however, the relevant UK authorities typically are reluctant to advise whether a particular disclosure will qualify as a protected disclosure under PIDA.

In 2014, the FCA and the Bank of England Prudential Regulation Authority carried out research on the impact of financial incentives to encourage whistle-blowing in the United States. They found no empirical evidence of incentives leading to an increase in the number or quality of disclosures received and believed that incentives could undermine effective internal whistle-blowing mechanisms. A response by the Department for Business, Innovation and Skills to a whistle-blowing consultation the same year set out the UK government’s view that incentives should not form an integral part of the whistle-blowing framework. At present, only the CMA offers financial incentives for information on cartel activity and payouts are discretionary.

III ENFORCEMENT

i Corporate liability

Save when otherwise provided by statute, a corporate will be liable for the offences it commits just as it would be if it were an individual. As a corporate can act only through natural persons, liability is based on acts committed by its respective officers or employees in the course of employment. Liability is attributed through one of two means: vicarious liability or the identification principle.

Vicarious liability typically, but not invariably, arises from the commission of a strict liability offence, namely offences that do not require fault or intention on the part of the offender. Such offences are usually created by statute and are most common in quasi-regulatory areas of criminal law, such as health and safety and trading standards.

The ‘identification principle’ is, by contrast, fault-based and attributes to the company the acts and state of mind of those who represent the company’s directing mind and will. The identification principle does not attribute to the company the acts and state of mind of all employees but only those who are serving on the company’s board of directors, the managing director and other superior officers carrying out management functions.

Because of the limited number of strict liability offences, most corporate prosecutions in the United Kingdom are based upon – and require application of – the identification principle. That often poses significant difficulty to prosecutors. The larger the company or the more diffuse its corporate structure, the more difficult it often is to attribute liability to the company. That has prompted widespread criticism of the identification principle, including by the Director of Public Prosecutions in relation to the ‘phone hacking’ scandal when the absence of corporate prosecutions was laid at the door of the identification principle.

30 The Director of Public Prosecutions stated that ‘the law on corporate liability in the United Kingdom makes it difficult to prove that a company is criminally liable if it benefits from the criminal activity of an...
Green QC, the former director of the SFO, had also expressed his preference that the test for corporate criminal liability be reconsidered, lamenting that email trails tend to dry up at a fairly junior level.31

One response to these difficulties has been the introduction of the ‘failure to prevent’ model of liability adopted in Section 7 of the BA with respect to bribery and, more recently, Part III of the Criminal Finances Act 2017 (CFA) with respect to facilitation of tax evasion offences. In 2017, the UK government conducted a consultation on possible reform of corporate criminal liability.32 Several possibilities were proposed in the consultation document, including (1) amending the identification principle by broadening the scope of those regarded as a directing mind of a company, (2) creating a new strict liability offence based upon principles of vicarious liability and (3) creating a new strict direct liability offence that focuses on the responsibility of a company to ensure that offences are not committed in its name. The consultation document also discussed the possibility of expanding the failure to prevent model to include other economic crimes. Economic crimes that might fall within any such future offence include conspiracy to defraud, false accounting and the fraud offences set out in Section 1 of the Fraud Act 2006 (FA06). If the proposed reforms were to be adopted, they would be likely to make corporate prosecution simpler. The UK government has not yet announced any definitive plans or legislative proposals to reform corporate criminal liability.

As regards representation, when both the corporate and its employees are being investigated, typically they are not represented by the same counsel. While joint representation sometimes occurs at the beginning of an investigation, the interests of the corporate and the corporate’s employees often diverge early in the investigation, requiring separate representation. The costs of an individual’s representation may be covered by director and officer liability insurance, although it is common for such policies to require any funds that are dispensed to be returned if the recipient of the funds ultimately is convicted of a criminal offence.

Individuals do not always have the right to legal representation at an interview, even when the interview occurs in a criminal context. By way of example, when a representative of the SFO is interviewing an individual pursuant to the SFO’s powers under Section 2 of the CJA87, the SFO is not required to permit a solicitor to be present at the interview or wait for one to arrive before beginning the interview. Similarly, since the Divisional Court’s decision in R (Lord, Reynolds and Mayger) v. Serious Fraud Office,33 the SFO has been empowered to – and often does – exclude company lawyers from attending employee interviews (even over the employee’s objection).

By contrast, individuals have the right to legal representation when being interviewed as a criminal suspect. In such circumstances, the PACE Code of Conduct gives individuals the right to consult and communicate privately with a solicitor at any time during the interview, conducted during their employment’. CPS Blog, ‘No further action to be taken in Operations Weeting or Golding’ (11 December 2015), www.cps.gov.uk/news/latest_news/no_further_action_to_be_taken_in_operations_weeting_or_golding, accessed 11 May 2018.


Interviews usually are carried out at a police station following arrest, although certain authorities – such as the SFO – often insist upon conducting the interviews on the SFO's own premises.

Other rights and duties of an individual being interviewed in a criminal context likewise depend upon the individual’s status. The target of a criminal investigation can generally decline to answer the questions put to him or her, but an individual being interviewed as a witness must answer any and all questions that are asked.

If a target of a criminal investigation exercises his or her right to remain silent when being interviewed but provides at trial a response on which the target seeks to rely in defence, the court may draw an adverse inference from the target’s silence during the interview. By contrast, a response that an individual who was not a target was required to provide when being interviewed generally cannot be used against that individual in a subsequent criminal prosecution.

**ii Penalties**

Sanctions for corporate misconduct have become increasingly severe in England and Wales with nominal fines or non-criminal, regulatory outcomes no longer being guaranteed. There has been a sea change in recent years in the approach taken by many UK prosecutors to corporate offending, with substantial financial penalties and other severe criminal consequences seeming to increase with each passing year.

The FCA collected a total of £22,216,446 in fines during 2016 for regulatory breaches, a significant drop from the previous year. However, the total fines levied by the FCA in 2017 rose to £229,515,303, an increase that is primarily attributable to Deutsche Bank’s £163,076,224 settlement with the FCA in relation to the failings in the bank’s anti-money laundering systems. However, regulatory fines and criminal prosecutions are only two of the FCA’s many disciplinary and enforcement powers. The FSMA gives the FCA power to impose a range of regulatory sanctions on those it regulates, from mere public censure at one end to the suspension or cancellation of FCA authorisation and the imposition of substantial regulatory fines at the other.

The FCA’s Decision Procedure and Penalties Manual sets out a non-exhaustive list of factors the FCA should consider when determining what action to take in a particular matter. These include the nature, seriousness and impact of the suspected breach, the conduct of the firm or approved person after the breach occurred or was discovered (including how quickly, effectively and completely the breach was brought to the FCA's attention), the disciplinary record and compliance history of the firm or approved persons, any published guidance by the FCA and any action taken by the FCA in similar cases. In addition, the FSMA gives the FCA power to prosecute criminal offences, such as insider dealing, pursuant to the Criminal Justice Act 1993 (CJA93) and breaches of the Money Laundering Regulations 2017 (MLR17).
Like the FCA, the CMA has both civil and criminal powers with respect to competition law infringements. The civil remedies available to the CMA range from settlement, accompanied only by the making of certain commitments, to the imposition of financial penalties. Settlement is a voluntary process\(^\text{37}\) pursuant to which the infringing firm makes an unequivocal admission of liability and in return may receive a discount of up to 20 per cent of the penalty that otherwise would have been imposed. Commitments and directions are agreements between the firm and the CMA that, if not complied with, can be enforced through the courts.\(^\text{38}\)

Commitments are accepted by the CMA only when the CMA deems, \textit{inter alia}, its concerns to be capable of being fully addressed by the commitments. Similarly, directions are imposed only if the CMA is of the view that they are sufficient to end the particular infringement.\(^\text{39}\) The most significant civil power at the CMA’s disposal is the power to impose financial penalties of up to 10 per cent of a firm’s worldwide turnover in the business year preceding the date on which the CMA makes its decision.\(^\text{40}\)

The CMA and the SFO can both criminally prosecute individuals who are suspected of having committed a cartel offence.\(^\text{41}\) By contrast, they can impose upon corporates only civil sanctions for anticompetitive conduct. Whether that will continue to be so remains to be seen, despite the criticism that appears to be growing in the United Kingdom of the traditional limitations on corporate criminal liability.

The SFO is responsible for prosecuting serious or complex fraud, bribery and other forms of corruption. It has two options for resolving such conduct in the case of corporates: entry into a DPA or a criminal prosecution. DPAs were introduced in the United Kingdom in February 2014\(^\text{42}\) as a discretionary tool enabling prosecutors to enter into agreements with offending corporates, under the supervision of a judge, to suspend prosecution for a defined period of time so long as the corporate meets specified conditions during that time.

The use of DPAs looks likely to increase, with three having been entered into by the SFO in respect of bribery and corruption in the \textit{Standard Bank}, \textit{XYZ} and \textit{Rolls-Royce} cases. In addition, a DPA was agreed in 2017\(^\text{43}\) between the SFO and Tesco Stores Limited following an investigation into accounting practices at Tesco that led to profits being overstated by £326 million. The fines levied in the \textit{Rolls-Royce} and \textit{Tesco} cases alone totalled £368,075,145 (not including the disgorgement of profits in the \textit{Rolls-Royce} case).

The Joint SFO and CPS Deferred Prosecution Agreements Code of Practice makes it clear that the SFO is ‘first and foremost’ a prosecutorial authority and that the SFO and the CPS will offer a DPA instead of pursuing a full prosecution only in exceptional cases.\(^\text{44}\)

The public interest factors that prosecutors are supposed to take into account when coming

---

37 Historically, settlement took place informally. Section 42 of the Enterprise and Regulatory Reform Act 2013, however, introduced a formal settlement procedure.
38 Competition Act 1998 (CA98), Sections 31E and 34.
39 CA98, Sections 32 and 33.
40 CA98, Section 36(8) and Competition Act 1998 (Determination of Turnover for Penalties) Order 2004, SI 2000/309.
41 Enterprise Act 2002, Section 188.
42 Pursuant to Schedule 17 of the Crime and Courts Act 2013
to such a decision include the corporate’s history of similar conduct, whether the conduct being addressed is part of the corporate’s established business practices, whether the corporate had an effective compliance programme and whether the corporate self-reported the matter within a reasonable period after the offending conduct was discovered.\textsuperscript{45} Importantly, the court is involved throughout the DPA process and ultimately must approve any DPA that is proposed.

Criminal prosecution or resolution of offending by means of a DPA can have a significant effect on the corporate from a public procurement perspective. The Public Contracts Regulations 2015\textsuperscript{46} provide for mandatory debarment when a corporate is convicted of certain criminal offences, such as the active bribery offences in Sections 1, 2 and 6 of the BA (although not the failure to prevent bribery offence in Section 7 of the BA). Mandatory debarment can sometimes be avoided if the corporate is able to demonstrate that it has adequately remediated the offending conduct. Absent such a showing, however, a criminal conviction triggers mandatory debarment. By contrast, entry into a DPA does not trigger mandatory debarment. Discretionary debarment may be ordered, however, depending upon the circumstances surrounding the DPA as well as in relation to any violation of Section 7 of the BA.

Corporate tax offences are resolved largely by HMRC, in line with its applicable Code of Practice, by means of a civil resolution.\textsuperscript{47} Factors that may contribute to a criminal outcome include a suspicion of deliberate concealment, deception, conspiracy or corruption or when there is a link to suspected wider domestic or overseas criminality.

Violations of the financial sanctions regime may lead to the imposition of a monetary penalty by the OFSI. Under the newly enacted PCA, the OFSI can impose a monetary penalty of up to £1 million on a person if it is satisfied that, on the lower civil standard of probabilities, the person breached or failed to comply with the financial sanctions regime. When the breach or failure relates to particular funds or economic resources and it is possible to value them, the maximum fine permitted is the greater of either £1 million or 50 per cent of the estimated value of the funds or resources. As such, when it is possible to put a value on the breach, the fine could well be significantly more than £1 million.

\textbf{iii Compliance programmes}

The existence of an effective compliance programme can be relevant to both liability and penalty, depending on the circumstances. While the existence of adequate procedures is a defence to the corporate offence of failing to prevent bribery in Section 7 of the BA, it nonetheless also may be taken into account when considering the issue of penalty.

Section 7 of the BA provides for a defence to the corporate offence of failing to prevent bribery by persons associated with a corporate when the bribery is intended to obtain or retain a business advantage for the corporate. The defence requires that the corporate has adequate procedures designed to prevent persons associated with it from engaging in bribery. To be deemed adequate, the procedures must accord with the six principles set out in the

\textsuperscript{45} Ibid., Section 2.8.
\textsuperscript{46} The Public Contracts Regulations 2015, SI 2015/102, Regulation 57.
\textsuperscript{47} Her Majesty’s Revenue and Customs (HMRC), ‘Code of Practice 9: HM Revenue & Customs Investigations where we suspect fraud’, (HMRC Digital Service, June 2014).
Ministry of Justice’s (MOJ) guidance on the BA\(^48\) – proportionality, top-level commitment, risk assessment, due diligence, communication (including training), and monitoring and review. These are overarching principles and, as such, each set of procedures must be tailored to the individual corporate.

To date, no corporate has relied successfully upon the adequate procedures defence. The three DPAs entered into by the SFO thus far all have required changes to be made to the company’s existing policies and procedures: Standard Bank agreed to commission an independent review of its anti-bribery and corruption controls, policies and procedures and XYZ agreed to carry out a review and submit annual compliance reports to the SFO. While Rolls-Royce some years earlier had hired Lord Gold to conduct an independent review of its compliance procedures, the terms of its DPA called for the company to complete the implementation of a compliance programme adhering to the review recommendations as well as the continued retention of Lord Gold as an independent specialist adviser.

In early 2018, the CPS brought a successful Section 7 prosecution against Skansen Interiors Limited, a refurbishment contractor with approximately 30 employees operating in England out of a small open office in London, in connection with bribes paid by a managing director to secure a £6 million contract with a developer in Manchester. After the company conducted an internal investigation, dismissed the implicated employees, adopted an anti-corruption policy and self-reported to and cooperated with the enforcement authorities, it was charged under Section 7 of the BA. At trial, Skansen argued that because, among other things, it espoused certain ethical corporate values, had adopted certain financial controls and had standard anti-bribery clauses in its contracts, it had in place adequate procedures in light of its small size and limited operational reach. The jury was not convinced and convicted the company. Because at the time of trial the company was dormant and had no assets, the only available sentence was absolute discharge. Indeed, it is reported that the CPS did not offer Skansen a DPA because it was a dormant company that was unable to pay a fine.\(^49\)

Camilla de Silva, the SFO’s Joint Head of Bribery and Corruption, has stated that Skansen’s prosecution was a ‘salient reminder’ that a ‘high bar’ will need to be reached for an adequate procedures defence to succeed and that the starting point is to have substantial and bespoke compliance procedures that actually work.\(^50\) The case does provide an important reminder for all companies – no matter the size of their operations – to ignore anti-bribery compliance at their own peril. Beyond that, because juries do not provide an explanation of their verdict, it is difficult to draw any concrete conclusions about the scope of the adequate procedures defence from this case. However, there remains a lingering sense of unease and confusion about the decision by the CPS to bring a prosecution against a company that had self-reported and apparently cooperated extensively with the enforcement authorities, including by waiving privilege over certain documents, simply to send a message to others.

---


The CFA also provides that a company will have a defence to tax evasion facilitation offences if it maintains prevention procedures that are reasonable in all circumstances. While the concept of reasonable prevention procedures in the CFA appears to be distinct from adequate procedures in the BA at first sight, the HMRC guidance in relation to the CFA offences confirms that the reasonableness of the prevention procedures will be assessed against the same six principles referred to in the MOJ guidance on the BA.  

As regards competition offences, the CMA’s Penalty Guidance makes it clear that compliance activities can merit in particular cases a penalty discount of up to 10 per cent. The starting point in that regard is neutral so that the mere existence of compliance efforts will not necessarily be treated as a mitigating factor. Evidence of adequate steps being taken to achieve a clear and unambiguous commitment to competition law compliance throughout the organisation (from the top down), and appropriate steps having been taken relating to competition law risk identification, risk assessment, risk mitigation and review activities, are often treated as mitigating factors.  

For firms regulated by the FCA and therefore bound by the provisions of the FCA Handbook, the establishment and maintenance of effective systems and controls for compliance with applicable requirements and standards, and for countering the risk of the firm being used to further financial crime, is mandatory. When a firm has not adopted such measures, it should expect to incur liability that is commensurate with the inadequacy of the measures it has taken. In fact, the FCA has sometimes penalised firms for not having established effective compliance systems and controls even in the absence of any other misconduct.

iv Prosecution of individuals  
When a corporate is prosecuted, it is usual in England and Wales for enforcement action to be taken against culpable individuals too. Guidance, such as that setting out the common approach of the CPS and the SFO (and formerly the prosecutorial arm of HMRC), makes it clear that prosecution of a company is not a substitute for prosecution of criminally culpable individuals such as directors, officers or employees. When considering whether to offer a DPA to a company, the prosecuting authority is bound to opt for prosecution

---

53 FCA Handbook, SYSC 3.2.6R and SYSC 6.1.1R.  
54 In November 2015, the FCA fined Barclays Bank plc £72.6 million for failing to minimise the risk of being used to facilitate financial crime. In doing so, the FCA found that the bank had arranged and executed a £1.88 billion transaction for numerous ultra-high net worth politically exposed persons without conducting adequate due diligence or establishing the purpose and nature of the transaction. Importantly, the FCA did not find that the funds at issue had been produced, in whole or in part, by underlying criminal activity. The FCA nonetheless fined Barclays Bank plc for regulatory failings. See FCA, ‘Final Notice to Barclays Bank Plc’ (25 November 2015).  
if it considers that the company has attempted to shield culpable individuals or withheld material that could jeopardise an effective investigation against them. The reason cited for that policy is that prosecution of culpable individuals provides a strong deterrent against future corporate wrongdoing. For example, while Tesco has agreed a DPA with the SFO, three former company directors are due to stand trial in September 2018 on fraud and false accounting charges. When enforcement action is taken against an individual, it can pose a number of issues for the corporate involved. In particular, corporates must be mindful of any employment law obligations they owe towards such employees and ensure that any action they take against them is commensurate with the misconduct that has been identified.

The most common step taken against employees suspected of wrongdoing during the course of an investigation (whether internal or external) is suspension. The timing of the suspension must be considered carefully, however, as suspension for the entire duration of an investigation may not be deemed to be fair and reasonable from an employment law perspective. Suspension therefore usually occurs only after the particular employee has been interviewed as a suspect or charges have been made against that individual.

Although there is no requirement for corporates to pay for an individual’s legal representation (save for any provisions to the contrary in the individual’s employment contract), it is common for corporates to do so in the early stages of an investigation. As the majority of those charged tend to be senior officers of a corporate – namely, those constituting its controlling mind and will – these individuals are often able to rely upon director and officer liability insurance, which may provide cover until the individual is found to be guilty or otherwise at fault (see above).

The recent case of R (on the application of AL) v. Serious Fraud Office brought to the fore the tensions that can arise when the SFO brings a prosecution against employees of a company that has secured a DPA with the SFO (in this case, XYZ) and the employees attempt to rely in their defence on information over which the company seeks to claim privilege, but which may be relevant to employees’ defence. In this case, the defendants challenged the failure of the SFO to compel XYZ pursuant to the ongoing cooperation and disclosure terms of the DPA to surrender interview notes made by the company’s lawyers during interviews with the defendants and other employees. The SFO requested the interview notes from XYZ, but the company refused to disclose them, citing privilege. The SFO did not accept the argument on the basis of recent developments in English law on privilege (see discussion in Section IV.iii), but ultimately relented. Although the court refused the defendants’ application on other grounds, it nonetheless issued a stark rebuke of the SFO’s failure to comply with its duty as a prosecutor to take reasonable steps to obtain the interview notes (including in light of the strong position that the SFO was in to challenge XYZ’s privilege claim) thus jeopardising the defendants’ right to a fair trial. Given the uncertainty already surrounding privilege over interview notes, the SFO may now be even more reluctant to accept oral proffers or summaries from companies wishing to secure a DPA, as the proffers or summaries may be deficient evidence when it comes to pursuing culpable individuals.

IV INTERNATIONAL

i Extraterritorial jurisdiction

Typically, jurisdiction over criminal conduct is state specific. A state will usually have jurisdiction only when some or all of the offence takes place within its territory or the accused or victim is a national of that state. The exception is when principles of universal jurisdiction apply, such as in relation to war crimes, or the relevant jurisdiction has enacted laws with extraterritorial effect.

In the United Kingdom, it is well established that statutes are not to be interpreted as having extraterritorial effect unless they expressly state otherwise. In recent years, a number of such statutes have been enacted. The effect of this is that UK authorities, depending on the circumstances of the particular case, may prosecute offences that took place overseas, whether wholly or in part, when there is some connection to the United Kingdom, such as through incorporation, nationality or residency.

Key offences with extraterritorial effect include:

a fraud under the FA06;

b dishonesty under the CJA93;\(^{58}\)

c terrorism under the Terrorism Act 2000 and Terrorism Act 2006;

d bribery under the BA;

e money laundering under the POCA; and

f tax evasion facilitation offences under the CFA.\(^{59}\)

The BA has exceptionally broad extraterritorial effect. Corporates that carry on a business or part of a business in the United Kingdom may incur liability under Section 7 for bribery committed anywhere in the world for their benefit by persons associated with them, irrespective of whether those persons have any other connection to the United Kingdom. Liability for both UK incorporated companies as well as those that merely carry on business or a part of a business in the United Kingdom therefore extends to acts committed on their behalf abroad.

The CFA may be deemed to have broad extraterritorial effect. Corporates that carry on a business or part of a business in the United Kingdom may incur liability under Part III thereof for tax evasion facilitation offences committed anywhere in the world by persons associated with them, irrespective of whether those persons have any other connection to the United Kingdom.

In relation to money laundering, Part 7 of the POCA makes it clear that liability for money laundering offences may be predicated on criminal conduct that occurred abroad. The only additional requirements are that such overseas criminal conduct constituted a criminal offence in the United Kingdom when it occurred and proceeds of the overseas criminal conduct have been transferred, in some manner, to the United Kingdom.

---

\(^{58}\) Part I of the Criminal Justice Act 1993 applies to the sections of the Theft Act 1968 that have not been repealed.

\(^{59}\) Part III of the Criminal Finances Act 2017 (CFA).
The BA, the CFA and the POCA are part of a trend in UK law to provide liability for offences taking place abroad. It remains to be seen whether this trend will continue following the conclusion of the UK government consultation on reforming corporate criminal liability, which also discusses the possibility of expanding the failure to prevent model to include other economic crimes.

ii International cooperation

With the internationalisation of business, it is becoming more and more common for cases to involve criminality or participants in more than one jurisdiction. Law enforcement and prosecutorial authorities are increasingly dealing with that challenge through a variety of formal and informal channels.

The United Kingdom has enacted a number of statutes to facilitate the sharing of information between and among domestic and overseas authorities for the investigation and prosecution of crime. These information gateways include Part XXIII of the FSMA, which permits the disclosure of confidential information for the purpose of allowing the performance of a public function, and Section 68 of the Serious Crime Act 2007, which permits public authorities to disclose information to other organisations to prevent fraud.

A number of memoranda of understanding (MOUs) exist between the various UK authorities and with their international counterparts. Domestic examples include the MOU on Tackling Foreign Bribery, of which the FCA, the SFO, the NCA and the City of London Police are signatories, the MOU between the CMA and the SFO, and the MOU between the CMA and the FCA in relation to concurrent competition powers. One international example is the MOU between the FCA and the SEC.

In addition to domestic statutes and MOUs, the United Kingdom has signed a number of multilateral and bilateral mutual legal assistance (MLA) treaties enabling prosecuting authorities to obtain evidence overseas. These include the European Convention on Mutual Assistance in Criminal Matters 1959, the Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union 2000, the United Nations Convention against Corruption 2003, the Commonwealth Scheme Relating to Mutual Assistance in Criminal Matters (1986) and various bilateral agreements with individual countries such as the United States. Section 7 of the Crime (International Co-operation) Act 2003 also provides for UK prosecutors to obtain overseas evidence through letters of request.

In addition to the formal means of information gathering mentioned above, law enforcement authorities can draw upon an array of informal information exchange networks. It is not uncommon for UK authorities to speak informally with their foreign counterparts. Issues of forum and investigation primacy tend to be resolved following informal discussions, particularly in reasonably straightforward or uncomplicated cases. More complicated cases may require prosecutors to engage the more formal MLA means of information exchange.

As a result of the foregoing measures, corporates being investigated in one jurisdiction should be conscious that information regarding the investigation, especially if touching other jurisdictions whether through relevant conduct or some other territorial nexus, will often be made available to law enforcement or prosecutorial authorities overseas. China, to cite only one example, recently initiated a bribery prosecution of a company that had previously been convicted of bribery in China by an overseas prosecutor.
A further possible consequence of MLA arrangements between states is the extradition of individuals. Two types of extradition exist in the United Kingdom: import extradition and export extradition. The former relates to a request to another state for the extradition of a person to the United Kingdom. The latter relates to a request by another state for the extradition of someone from the United Kingdom. Importantly, not all offences are extraditable offences.

The Extradition Act 2003 (the 2003 Act) regulates both import and export extradition. Part 1 of the 2003 Act regulates export extradition to category 1 states. These are EU Member States that have implemented the European Arrest Warrant mechanism. For the most part, dual criminality is required to be shown in that the conduct at issue must constitute an offence in the United Kingdom as well as in the state seeking extradition. Part 2 of the 2003 Act regulates export extradition to category 2 states – that is, to non-EU Member States.

Decisions regarding extradition to non-EU Member States are made by the UK Secretary of State. Various restrictions apply to extradition from the United Kingdom, such as whether the death penalty might be imposed or whether extradition to a third state could ensue following initial extradition. Import extradition is regulated by Part 3 of the 2003 Act. As with export extradition, the applicable mechanism for import extradition generally depends upon whether the relevant state is category 1 or 2. Whether such requests are granted is determined ultimately, of course, by the overseas state.

iii Local law considerations

One of the central issues in cross-border investigations, especially those involving the United States, is the application of the UK data protection regime. The General Data Protection Regulation prohibits the transfer of personal data from the United Kingdom outside the European Economic Area unless the recipient, jurisdiction or territory is able to ensure a UK-equivalent level of protection to those to whom the data belong. Whether a jurisdiction or territory is deemed to provide an adequate level of protection is decided by the European Commission.60

Until 2015, personal data were permitted to be transferred to certain US companies that had agreed to adhere to the Safe Harbour framework agreed between the European Commission and United States. But the Court of Justice of the European Union (CJEU) invalidated the Safe Harbour framework in October 2015 in Maximillian Schrems v. Data Protection Commissioner.61

In July 2016, the European Commission adopted the EU–US Privacy Shield, a replacement for the Safe Harbour regime that imposes obligations on US companies to protect EU citizens’ personal data in accordance with certain principles, including the tightening of conditions for onward transfer of data to third parties and clear safeguards and transparency obligations on access by the US government. However, there have been lingering concerns about the domestic surveillance programmes operated by the US government

---


61 Case C-362/14.
and their interference with the data of EU citizens. The Irish High Court has concluded that the Privacy Shield has been unable to eliminate those concerns and has submitted preliminary reference to the CJEU asking it to decide questions affecting the validity of the Privacy Shield.

Legal professional privilege is another issue that must be considered from the beginning of an investigation. England and Wales recognises both legal advice privilege and litigation privilege in relation to advice provided by both in-house and external counsel, with one exception in relation to competition law.

It has become increasingly common for authorities to seek the production of investigation materials, arguably subject to legal professional privilege, such as first account witness interviews, as a sign of cooperation. There are substantial difficulties with invoking privilege over such documents.

In 2016, the High Court issued an important decision on the unavailability of legal advice privilege in Re the RBS Rights Issue Litigation. The court upheld the restrictive approach to defining a ‘client’ that was adopted in Three Rivers (No. 5) and rejected claims of privilege asserted by RBS over notes of internal interviews on the grounds that the pertinent group of employees and ex-employees did not constitute the client for the purpose of privilege. Consequently, the information provided by that group of RBS employees and ex-employees did not fall within the scope of legal advice privilege. The contention that the interview notes could still fall within the scope of legal advice privilege on the basis that they were ‘lawyers’ working papers’ was also rejected by the court.

The decision of the High Court in the ENRC case further increased the difficulty in invoking privilege over litigation materials. The court ordered ENRC to hand over various documents to the SFO, rejecting a claim of litigation privilege in respect of most of the pertinent materials. The court’s view was that litigation privilege required the company to be aware of circumstances that made prosecution a real likelihood as opposed to a mere possibility. The company’s fear of a dawn raid and subsequent prosecution by the SFO was held to be insufficient to establish that prosecution was a real likelihood. Consequently, the court concluded that litigation privilege did not protect the majority of the documents sought by the SFO.

The decision in ENRC can be compared with the approach taken by Lord Justice Vos in the December 2017 case of Bilta (UK) Ltd (in liquidation) and others v. Royal Bank of Scotland and another. The court took the view that documents created by RBS during an internal investigation were covered by litigation privilege as they were created for the sole or dominant purpose of expected tax litigation with HMRC. Vos LJ took care not to draw a general principle from the approach taken in ENRC and instead emphasised the importance of taking a realistic and commercial view of the facts. In that regard, His Lordship appears to have been swayed by, among other things, the fact that RBS commenced its internal investigation after

---

62 The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (High Court of the Republic of Ireland, unreported judgment of Ms Justice Costello, 3 October 2017, [2016 No. 4809 P]).
63 Ibid., unreported request for a preliminary ruling by Ms Justice Costello, 12 April 2018, [2016 No. 4809 P]).
64 [2016] EWHC 3161 (Ch).
66 Bilta (UK) Ltd (in liquidation) and others v. Royal Bank of Scotland and another [2017] EWHC 3535 (Ch).
receiving a notice from HMRC of its decision to commence tax assessment. Notwithstanding the care taken to distinguish ENRC on the facts, however, the two decisions appear to be in tension with one another.

The foregoing decisions will doubtless generate much debate as to how best to protect notes of internal investigation interviews and other investigation materials from disclosure. ENRC is seeking to appeal the decision of the High Court, and the Court of Appeal is due to hear the case in Summer 2018. Unless the Supreme Court hears the issues raised by these cases, it is likely that real difficulty in invoking legal professional privilege will remain.

V YEAR IN REVIEW

Having so far survived a pledge by the ruling Conservative Party to merge it with the NCA, the SFO has continued its aggressive enforcement of the BA and other corporate crimes. In early 2017, the SFO completed its £497.25 million DPA with Rolls-Royce and £129 million DPA with Tesco and secured convictions against FH Bertling Ltd and seven of its employees in relation to bribery in Angola. At the same time, the SFO continues its probe into the alleged corrupt conduct by Airbus and Unaoil. A number of other companies have become embroiled in the Unaoil investigation, with the Swiss engineering company ABB, the US engineering and construction company KBR and UK oil services group Petrofac among the corporates now also the subject of SFO investigations. The SFO has also opened new investigations into alleged corrupt conduct by household names such as Rio Tinto, Amec Foster Wheeler and British American Tobacco.

There have been significant legislative developments, with the entry into force of the CFA introducing two new corporate criminal offences concerning the facilitation of tax evasion, and the PCA empowering the OFSI to impose financial penalties in respect of violations of the sanctions regime. These developments, with the UK government’s consultation on the reform of corporate criminal liability, raise the possibility of an uptick in investigations and enforcement actions focused on corporates in the coming few years.

The CFA has also given powerful tools to the SFO and the NCA to counter money laundering, such as the unexplained wealth order (UWO). An UWO requires a person who is reasonably suspected of involvement in, or of being connected to a person involved in, serious crime to explain the nature and extent of their interest in particular property – and to explain how the property was obtained – when there are reasonable grounds to suspect that the respondent’s known lawfully obtained income would be insufficient to allow the respondent to obtain the property. An UWO is an investigative tool; it is not, in itself, a power to recover assets. However, if the respondent fails to provide an explanation, the asset will be presumed to be recoverable. In early 2018, the NCA obtained UWOs against two properties totalling £22 million, which are believed to be owned by a Central Asian politician.

The past year also saw the promulgation of the MLR17, which gives effect to the European Union’s Fourth Anti-Money Laundering Directive. The MLR17 is more prescriptive than its predecessor and provides additional detail on the customer due diligence measures required to be taken by regulated entities, an expansion in the definition of politically exposed persons, a requirement for regulated firms to conduct a money laundering risk assessment

---

© 2018 Law Business Research Ltd
and the creation of new criminal offences for prejudicing investigations into a breach of the MLR17 or making false or misleading statements pursuant to a requirement imposed under the MLR17.

Finally, the decision of the High Court in ENRC will have important ramifications for litigation privilege in the United Kingdom, rendering it harder for corporates to advance arguments that litigation privilege applies to documents prepared during the course of an internal investigation and requiring lawyers to give even greater thought to how best to preserve privilege for their clients during the course of future investigations.

VI CONCLUSIONS AND OUTLOOK

Tackling corporate crime has become a key political priority for the United Kingdom in recent years. With it has come a raft of legislative measures aimed at providing additional routes to corporate liability and tougher sentencing.

The CFA created a new corporate criminal offence of failing to prevent an associated person from facilitating UK or foreign tax evasion – offences based on the strict liability ‘failure to prevent’ model used in the Section 7 BA offence. There is clearly a desire on the part of the UK government to tackle tax evasion and penalise those corporates deemed to be facilitating it. The desire to clamp down on broader economic crime is also evidenced in the United Kingdom Anti-Corruption Strategy 2017–2022, in which the government has pledged to consider possible expansion of the ‘failure to prevent’ model to other economic crimes in light of the findings from the 2017 consultation.

Similarly, the PCA has introduced extensive new provisions regarding financial sanctions breaches. Historically, very few prosecutions have been brought in the United Kingdom for breaches of financial sanctions. The PCA demonstrates the current UK government’s intention to change that by increasing the maximum term of imprisonment for breaches from two to seven years and providing a new civil monetary penalty regime operated by the OFSI. In 2017, OFSI received reports of 133 suspected breaches of sanctions reaching an aggregate value of approximately £1.4 billion. Although the OFSI is yet to impose any public penalties for sanctions violations, the recent overhaul of the sanctions enforcement regime suggests that the coming years may see increased enforcement action for breach of financial sanctions.

Following the departure of David Green QC, the SFO has announced his successor as Lisa Osofsky, a former lawyer at the Federal Bureau of Investigation and regional head of investigations at a global compliance firm. Ms Osofsky will determine the direction that the SFO takes with regard to corporate criminal prosecution, but that will undoubtedly be informed by the need for continuity and certainty. Armed with a ‘blockbuster’ budget, the new director will be required to tackle high-profile trials, such as the retrial of former Tesco executives in September 2018. Ms Osofsky also will need to oversee the closure of the investigation into Airbus (it is rumoured that the SFO has been in talks with Airbus about

68 Alexandra Rogers, ‘SFO in talks to change its funding arrangements for “blockbuster” cases’ (City A.M., 13 March 2018).
a billion-pound settlement)\textsuperscript{69} and the appeal in the ENRC case, which will have important ramifications for a prosecutor’s power to compel production of material that a company generates during the course of an internal investigation.

As the United Kingdom prepares to exit the European Union, Parliament passed the Sanctions and Anti-Money Laundering Act 2018 (SAMLA). The purpose of the SAMLA is to give power to the government to impose sanctions and anti-money laundering and counter-terrorism financing measures following the United Kingdom’s exit, as the European Union has predominantly legislated in that area. The SAMLA grants very wide powers to the government to impose sanctions, for example, to further its foreign policy objectives or to promote respect for human rights, democracy, the rule of law and good governance. The SAMLA suggests that the United Kingdom outside the European Union will cooperate with its European partners on sanctions, but may also pursue unilateral sanctions where the European Union is stalled because of internal divisions.

It is clear that the investigation and prosecution of corporate wrongdoing has gained significant momentum in the United Kingdom in recent years. There is significant appetite to continue to clamp down hard on economic crime through legislative means and the provision of additional enforcement tools to UK prosecutors. Whether the pertinent authorities can continue to build on that momentum will be one of the stories to follow during the next year or two.

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:

- the relative roles of prosecutors, judges and private attorneys;
- the importance of state actors in establishing the facts of a case;
- the relative absence of attributes of an ‘adversarial’ process such as cross-examination;
- the limited (but evolving) ability to negotiate with the investigating authority;
- the nature and use of testimonial and other kinds of evidence; and
- 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). Criminal violations are divided into three categories, which determine maximum sanctions, the courts involved and participants in the process. High crimes (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 each

---

1 Antoine Kirry is a partner, Frederick T Davis is of counsel and Alexandre Bisch is a senior associate at Debevoise & Plimpton LLP.
2 Both these codes are available in English at www.legifrance.gouv.fr/Traductions/en-English/ Legifrance-translations.
significant city throughout France. There is no jury trial. Misdemeanours (contraventions) 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: complex and important matters, which are referred to an investigating magistrate, and simpler matters, which are handled by the public prosecutor.

Investigating magistrates are found throughout France. In some instances they are teamed together in a group called a pôle; for example, the pôle financier 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 after the latter has conducted a preliminary investigation. 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 obligated 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. 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. Since the public prosecutor’s views nonetheless have significant weight, 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.

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


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.
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. Since 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). The trial of a regular crime will be before 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’, 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 will then review the facts as well as the law de novo and reach its own conclusion as to both. Appeals from an assize 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.

© 2018 Law Business Research Ltd
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.

Although most criminal investigations involving international matters are likely to be addressed by an investigating magistrate, overall more than 90 per cent of all criminal cases proceed on a simplified basis without one. 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 to build an evidentiary record. 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.

**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, practice 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, but in a landmark decision of 18 March 2015, the French Constitutional Court reversed that long-standing position. A law passed on 21 June 2016 now ensures that suspects of market abuses are subject to one type of

---

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 the possibility of an *a posteriori* review of the constitutionality of French laws. Prior to that time, the Conseil Constitutionnel reviewed the constitutionality of French laws exclusively prior to their promulgation. A constitutional question may now be raised in a trial court if the contested law is applicable to the pending litigation and if the question is new or serious, and has not already been reviewed by the Conseil Constitutionnel. If the law has already been reviewed by the Conseil Constitutionnel, there must have been a change in circumstance such that the law should be reviewed again. A constitutional question can be transmitted to the Conseil Constitutionnel via the Court of Cassation (supreme court for judicial matters) or the Council of State (supreme court for administrative matters).
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 face a maximum financial sanctions 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 5 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 by the Paris Court of Appeals 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 global profits, before taxes, for a legal entity enterprise. The calculation of an enterprise’s profit for the purpose of applying the sanction is based on the highest profit 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 is the general lack of statutory incentive to do so. 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 them 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. In December 2016, the legislature adopted the Sapin II

---

6 A further disincentive is the fact that, as noted below 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.
Law, 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 and laundering of the proceeds of tax fraud without a criminal conviction. This procedure is available only to legal entities. In none of the three CJIPs approved to date does it appear that the company in question self-reported by bringing a matter to the attention of the authorities before an investigation started. The absence of self-reports in those cases may be because they occurred in matters where investigations had already commenced before the Sapin II Law was adopted. However, because of the lack of statutory incentive to self-report, it remains to be seen if, in the future, companies will elect to do so before a formal investigation with an investigating magistrate is commenced.

ii Internal investigations

Internal investigations in the American 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.

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 (1) lawyers can participate in internal investigations, (2) that they may do so even with respect to their usual clients and (3) 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

9 For a general description of the challenges of doing 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.
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\(^\text{12}\) 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 other countries may violate the law.\(^\text{13}\) 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 1970 Hague Evidence Convention. While a formal procedure under that Convention may 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


\(^{13}\) 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 Department of Justice (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).
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.

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 law of March 2017 on the corporate duty of care,14 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.

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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{17} In March 2018, in another case of overseas corruption, the Court of Cassation 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.\textsuperscript{18}

\textbf{ii Penalties}

Both corporate and individual criminal penalties, whether financial or imprisonment, tend to be significantly lower than in the United States.

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 very low by US standards. As an example, 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.\textsuperscript{19} 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.

\textsuperscript{15} Versailles Court of Appeals, 29 November 2012, No. 11/00332.
\textsuperscript{16} Paris Court of Appeals, 7 January 2015, No. 12/08695.
\textsuperscript{18} Court of Cassation, 14 March 2018, No. 16-82.117.
\textsuperscript{19} Id.
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 annual turnover for the previous three years.

iii Compliance programmes
The Sapin II Law adopted in December 2016 fundamentally changed French law with respect to compliance programmes. The law established the French Anti-corruption Agency (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.20

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. But 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 divulgence 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.21

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 as 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.

21 Court of Cassation, 19 March 2014, No. 12-87.416.
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 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 mutual legal assistance treaties (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 among 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.\(^{22}\) 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,\(^{23}\) 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.


\(^{23}\) The CISA provision has been liberally interpreted by the European Court of Justice to protect against multiple prosecutions.
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 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.24

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 National Financial Prosecutor 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. The promulgation of the first CJIPs agreements have yet to define a clear path for French authorities to re-establish leadership in this field, but clearly reflect a commitment by French authorities to be much more active in pursuing crimes that touch French interests. In any event, it seems clear that the requirement that all but small companies adopt robust compliance programmes, an obligation that is being monitored by the AFA, is certainly a part of the French legal landscape.

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 visible commitment in France may change that analysis.

Ilias G Anagnostopoulos and Jerina (Gerasimoula) Zapanti

I

INTRODUCTION

The responsibility for investigation of corporate conduct lies with the regulatory and prosecuting authorities (depending on the subject of the investigation). Regulatory authorities have the power to investigate, within their scope, corporate conduct (e.g., the Hellenic Competition Commission for cartel offences), but responsibility for criminal prosecution of corporate conduct always lies with the Prosecutor’s Office (the Prosecutor) and any findings related to criminal offences are forwarded to the Prosecutor to decide on further proceedings.

The Prosecutor is responsible for initiating and supervising investigations that may be performed by other agencies, for example, the police or the Financial and Economic Crime Unit (SDOE).

Following a series of amendments in legislation, two separate prosecuting offices have been established 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.

Apart from the ease of access to information, both special prosecutor’s 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

---

1 Ilias G Anagnostopoulos is managing partner and Jerina (Gerasimoula) Zapanti is a lawyer at Anagnostopoulos.
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 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).

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.

Note that 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, since 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).

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, etc.) 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.

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).

Criminal liability is an exception when referring to a legal entity (a company) because of the fact that under Greek law, 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.
As regards joint representation by counsel, this 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:

- **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;
- **suspension of the company’s ability to participate in public tenders or to request public funding** – repeated misconduct may lead to a permanent ban;
- **suspension of the company’s activity for a period of time**, depending on the severity of the act; and
- **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 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

Major cases now in trial were initiated by internal corporate investigations in Greece and abroad. These cases mostly involve acts of fraud or corruption in relation to defence programmes and the supply of medical equipment. The findings of the internal investigations were included in reports, which were given to the prosecuting authorities and became the basis of the (initial) criminal investigations.

In addition, the Anti-Corruption Prosecutor’s Office has initiated two major investigations in relation to the questionable conduct of a pharmaceutical company and large-scale mismanagement related to the Hellenic Centre for Disease Control and Prevention. Both investigations are characterised by aggressive conduct by the authorities, including dawn raids, requests for assistance by other enforcement agencies, mutual assistance requests and releasing information to the public.
VI CONCLUSIONS AND OUTLOOK

It is expected that leniency or immunity procedures in criminal investigations, although not provided for all types of offences, will have a positive effect in exposing acts of corruption and money laundering. Note that 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.

A different approach (e.g., leniency and immunity provisions for entities) would encourage entities to report findings of their internal investigations to the authorities and deal more effectively with individuals involved in possible misconduct. It is also very important to find ways to manage on a central level (by communication between the authorities) the sanctions to be imposed in order to avoid sanctions for the same conduct in parallel and independent proceedings.
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.2 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 SFC3 and the HKCC4 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,5 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.6 In addition, the SFC can compel the production of documents and records7 and obtain a search warrant to search for and seize documents.8

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 2017 included corporate fraud and misfeasance, insider dealing, market manipulation,
intermediary misconduct, gatekeeping by sponsor firms and mis-selling of financial products. Accordingly, the SFC prioritised its resources by forming both permanent and temporary specialised teams, which helped it process increasingly sophisticated cases in a more efficient way as well as sharpening its expertise by addressing each of the key risks identified by its teams that have direct market contact.\(^9\)

Some regulatory agencies have published policies to encourage cooperation with their investigations. In December 2017, the SFC issued its ‘Guidance Note on Cooperation’ (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. In addition, the Competition Ordinance (Cap. 619) (Competition Ordinance) 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.

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)\(^10\) 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.\(^11\) 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.\(^12\)

In its Guidance on Cooperation, the SFC recognises voluntary and prompt self-reporting of any regulatory breaches or failings to it as a form of cooperation,\(^13\) 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,

---

10 The Joint Financial Intelligence Unit is a joint reach force between the Hong Kong Police Force and the Customs and Excise Department.
11 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).
12 See Paragraphs 4.3 and 4.4 of the Guidance on Cooperation.
13 See Paragraph 2.1 of the Guidance on Cooperation.
mere compliance with self-reporting obligations under the SFC rules\textsuperscript{14} will not amount to cooperation by itself.\textsuperscript{15} 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 forms,\textsuperscript{16} 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 Guidance on Cooperation.\textsuperscript{17}

The HKCC has also published a Leniency Policy for Undertakings Engaged in Cartel Conduct (Leniency Policy),\textsuperscript{18} which is meant to grant leniency to encourage self-reporting by companies that may have engaged in illegal activity, such as bid rigging or price fixing. The Leniency Policy provides that leniency is available only for the first member who reports the cartel conduct to the HKCC and meets all the requirements for receiving leniency. In exchange for a cartel member’s cooperation in the investigation of the cartel conduct, the HKCC will enter into an agreement with the undertaking not to take proceedings against it for a pecuniary penalty. The HKCC will also agree not to bring or continue proceedings in the Competition Tribunal or commence any other proceedings other than proceedings for an order under Section 94 of the Competition Ordinance declaring that the cartel member has contravened the First Conduct Rule.\textsuperscript{19} However, a leniency agreement offers no immunity from follow-on actions under Section 110 of the Competition Ordinance against cartel members by persons who can prove they have suffered loss or damage as a result of the cartel.\textsuperscript{20}

\textbf{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 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

\begin{footnotesize}
\begin{enumerate}
\item 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).
\item See Paragraph 3.1 of the Guidance on Cooperation.
\item 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 Guidance on Cooperation.
\item See Paragraphs 6.2 and 6.3 of the Guidance on Cooperation.
\item The First Conduct Rule prohibits an undertaking to (1) make or give effect to an agreement, (2) engage in a concerted practice or (3) as a member of an association of undertakings, make or give 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).
\item See Paragraph 1.7 of the Leniency Policy.
\end{enumerate}
\end{footnotesize}
evidence of which the SFC is otherwise unaware, including sharing the results of any internal investigation. However, if 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 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.

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 a leniency policy 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. 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.

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 Organised 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 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.

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

21 See Section 2 of Witness Protection Ordinance (Cap. 564).
22 See Section 7 of Witness Protection Ordinance (Cap. 564).
23 See Paragraph C.3.7 of Appendix 14 (Corporate Governance Code and Corporate Governance Report) of the Main Board Listing Rules.
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, 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. 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, 27 cold shoulder orders, 28 cease and desist orders, 29 disgorgement orders, 30 government costs orders, 31 SFC costs orders, 32 Financial Reporting Council costs orders 33 and disciplinary

---

24 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.
25 See Section 303 of the SFO.
26 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.
27 An order prohibiting a person from being involved in the management of specified corporations. See Section 257(1)(a) of the SFO.
28 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.
29 An order prohibiting a person from engaging in any specified form of market misconduct again. See Section 257(1)(c) of the SFO.
30 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.
31 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.
32 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.
33 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.
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;
b. suspension or partial suspension of the licence or registration;
c. revocation of approval to be a responsible officer;
d. suspension of approval to be a responsible officer;
e. a fine (up to HK$10 million or three times the profit gained or loss avoided, whichever is the higher); or
f. private or public reprimand.

The range of potential sanctions will vary 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 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 the Corruption Prevention 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

34 An order giving a copy of the report of the Market Misconduct Tribunal proceedings to any regulatory body that may take disciplinary action against the relevant person. See Section 257(1)(g) of the SFO.
35 See Section 213(2)(c) of the SFO.
36 See Section 213(2)(d) of the SFO.
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 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 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.38 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 outcome of any criminal proceedings against the employee arising out of or connected with his or her employment.39 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.

IV INTERNATIONAL

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.40

38 See Paragraph 3.1 of the Guidance on Cooperation.
39 See Section 11(c) of the Employment Ordinance (Cap. 57).
40 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.
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.\(^\text{41}\)

\section*{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 117 signatories\(^\text{42}\) 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.\(^\text{43}\) 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 MOU for the Mainland-Hong Kong Stock Connect and the MOU concerning futures dated December 2017.

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 29 jurisdictions under the Mutual Legal Assistance in Criminal Matters Ordinance (Cap. 525)\(^\text{44}\) 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.

\section*{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\(^\text{45}\) or the Prevention of Bribery Ordinance.\(^\text{46}\) Advance approval is needed from the SFC for disclosing relevant non-public information to foreign regulators. In addition,

---

\(^{41}\) See Section 8 of the Competition Ordinance (Cap. 619).

\(^{42}\) Up to 27 December 2017, see www.sfc.hk/web/EN/about-the-sfc/collaboration/overseas/iosco-mmou.html, last accessed on 16 May 2018.


\(^{45}\) See Section 378 of the SFO.

\(^{46}\) See Section 30 of the Prevention of Bribery Ordinance (Cap. 201).
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

Regarding the SFC’s work during 2017, the most important update to its rules relating to investigation and enforcement was in its Guidance on Cooperation. It replaced an older version that had been in force for over a decade. The new rules illustrate the SFC’s approach to assessing cooperation in a clearer way by providing updated and specific examples and introducing the three-stage mechanism in quantifying a leniency grant.

As regards the SFC’s enforcement actions, record fines of HK$497 million were imposed by the SFC, which can mainly be attributed to the HK$400 million fine against HSBC’s private banking unit; nevertheless, the remaining HK$97 million represented a 40 per cent year-on-year increase. The SFC has also strengthened its enforcement actions against firms with internal control failures relating to know-your-client or anti-money laundering requirements.

Another trend is the SFC’s growing efforts in promoting international cooperation. In January and July 2017, the SFC updated its MOU for exchange of information with the US Securities and Exchange Commission and the UK Financial Conduct Authority, respectively. In December 2017, cross-border cooperation between the SFC and the CSRC also stepped up, as evidenced by the refreshed MOU for exchange of information and investigatory assistance (Refreshed MOU). Moreover, with the support of the court, documentary evidence obtained by a search warrant for an investigation by the SFC in Hong Kong may be transmitted to the CSRC to assist the investigation in the PRC.

Another new development is the Manager-In-Charge (MIC) programme put forward by the SFC in April 2017. It requires companies to identify individuals with oversight of core functions and map out their responsibilities and reporting lines. While this regime was not primarily conceived as a tool for enforcement, it helps the SFC identify responsible individuals and hold them accountable in cases of wrongdoing. The SFC’s investigation teams can then hone in on individual culpability at the inception of any investigation. If the evidence supports it, the SFC will take civil or criminal action against culpable individuals. According to the SFC, many firms took the opportunity to strengthen their governance structures, and more than 10,000 individuals had been appointed as MICs as at March 2018.

In terms of the HKCC’s enforcement actions, 2017 was also a landmark year in that the HKCC brought the first two cases to the Competition Tribunal under the Competition Ordinance since it came into force in December 2015. The first case was initiated in March 2017 against five technology companies allegedly involved in bid-rigging activities in a tender for the supply and installation of an IT server system. The trial is due to be heard in

47 Court of First Instance of Hong Kong High Court, see Tang Hanbo v. The Securities and Futures Commission and another (HCAL 229/2016).
June 2018. The second case commenced in August 2017 and again relates to alleged breaches of the First Conduct Rule, in this case by 10 home decorating companies suspected of entering into a market sharing agreement and a price-fixing agreement when providing renovation services to tenants of a public rental housing estate. The trial for this case is also scheduled to be heard in June 2018.

In the first case mentioned above, the Competition Tribunal has already made a few important decisions in the preliminary proceedings. First, it laid down precedents for the treatment of confidential information. Mr Justice Godfrey Lam granted the confidentiality treatment sought by the HKCC regarding tender prices (which was recognised as commercial information of the respondents), the identities of current and former employees of the respondents and the tender receiver, and the identity of the complainant. Second, the Competition Tribunal held that evidence obtained under compulsion from an employee was admissible for incriminating his employer, who was under a separate notice of interview, thus limiting the scope of the anti-self-incrimination provision to a ‘direct use prohibition’ under Section 45 of the Competition Ordinance.

VI CONCLUSIONS AND OUTLOOK

In a report issued by the SFC in February 2018, five areas of misconduct have been identified as the SFC’s enforcement priorities for 2018: corporate fraud, insider dealing and market manipulation, intermediary misconduct, sponsor misconduct and money laundering. Corporate fraud, which remains the SFC’s top enforcement priority, will also draw the regulator’s attention to misconduct, such as issuing false or misleading financial statements, sponsor’s failures relating to initial public offering fraud, and failures to manage conflicts of interest by senior management of listed companies.

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.

Regarding a sponsor’s misconduct, the SFC’s investigations are extending to more sponsor firms and sponsor principals in 2018, alerting sponsors to maintain the highest standards and to perform due diligence with professional scepticism.

As regards anti-money laundering, following the amendments to the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615) that came into effect on 1 March 2018, the SFC also published two relevant guidelines in March 2018. It is very likely that 2018 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, the number of surveillance requests from the SFC to the CSRC for information about suspicious southbound transactions doubled in 2017. With the Refreshed MOU in place and the rolling out of the reform of Hong Kong’s listing regime in April 2018 (to attract emerging and innovative companies from mainland China to the Hong Kong capital markets), there is little doubt that the aforementioned cooperation will remain strong (if not grow stronger) in 2018, 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.

Another observation is that opportunities and challenges coexist in new economies. On the one hand, the new listing regimes in Hong Kong support new economy companies and pre-revenue biotech firms. On the other, the SFC has taken regulatory action against a number of cryptocurrency exchanges and initial coin offering issuers and alerted investors to their potential risks.53 As the Chairman of the SFC recently acknowledged, the dramatic turnaround of the SFC’s attitude regarding weighted voting rights in such a short period of time reflects the saying that ‘life is full of surprises’.54 It will thus be interesting to see if the opening of a window will result in more doors being closed – new economy companies may be subject to closer monitoring from regulators.

The coming year will also be a busy year for the HKCC. With its new leadership55 bringing enforcement experience from the US and the European Union, and a budget of HK$200 million allocated to litigation activity, the HKCC is well equipped to bring more frequent and higher profile enforcement actions in 2018. As for the type of cases, although the first two cases in 2017 focused on breach of the First Conduct Rule, the CEO of the HKCC stated that cartels are not the ‘sole enemy’ and they would actively seek to detect and halt abuses by large firms using their market power to erect barriers to entry or squeeze out competitors. 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. 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.

55 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.
I INTRODUCTION

The Companies Act 2013 (the Companies Act) changed the philosophy of corporate governance as traditionally understood in India. It brought in stringent standards and created a new offence of fraud (with a very broad and sweeping definition) that covers a variety of situations and extends liability to companies, their officers, key management persons (KMPs), auditors, directors, etc. Separately, more traditional offences relating to corporate conduct, such as bribery, money laundering, cheating, criminal breach of trust and criminal conspiracy, continue to apply.

The Serious Fraud Investigation Office (SFIO), the government’s white-collar crime investigation agency, was established under the Companies Act to investigate corporate fraud. The relevant sectoral regulators, including the Securities and Exchange Board of India in relation to capital markets and the Competition Commission of India (CCI) in relation to competition matters, also hold investigative powers. However, these investigating agencies do not have the power to prosecute or assist a separate prosecution wing for prosecuting individuals and companies.

Under the Indian federal structure, the power to investigate vests with central and state agencies. Agencies such the Central Bureau of Investigation (CBI), the Enforcement Directorate (within the Ministry of Finance) (ED), the Anti-Corruption Bureau of the state governments, apart from the Economic Offences Wing of police departments, are also empowered to investigate and prosecute corporate conduct that may be implicated in offences.

Statutory powers of investigation and inspection of premises, including seizures of books, papers and documents, have been provided for under taxation laws and corporate laws to aid information gathering and to prevent destruction of documents and evidence by companies under investigation. Similarly, under the Competition Act 2002 (the Competition Act) the director general also has wide search and seizure powers in connection with the investigation of an offence by the CCI.

The powers of these investigating authorities, acting through an investigating officer, include the power to arrest an individual and carry out search and seizure of premises that are suspected of containing evidence of crime or proceeds of crime. The ED, investigating
offences under the Prevention of Money Laundering Act 2002 (PMLA), has additional powers to provisionally attach ‘proceeds of crime’, which may be the property involved in the crime or any property into which the proceeds of crime have been converted.

In recognition of the need to instil complete transparency, the ombudsman under the Central Vigilance Commission has been given the power of superintendence over the CBI under the Central Vigilance Commission Act, 2003.

It is of utmost importance that any business under investigation fully cooperates with the authorities, of course, without needlessly compromising its rights. Failure to cooperate may have consequences, such as arrest, in the immediate term and, in the long run may affect defence. On balance, it is important to adopt some of the best practices, such as claiming legitimate privilege, confidentiality and right against self-incrimination. The KMPs and other officers of a business are required to appear personally before the investigating officer for interrogation, during which time, typically, constant access to lawyers is not allowed. An adversarial stand during investigation is risky from both commercial and individual points of view.

II CONDUCT

i Self-reporting

There is no express obligation *per se* on companies to self-report instances of internal wrongdoing or fraud. An external reporting mandate is imposed upon auditors, practising company secretaries performing a secretarial audit or upon a cost accountant who is performing a cost audit, each in accordance with the provisions of the Companies Act.

In terms of the Companies Act, the board of directors of a company is under an obligation to ensure that proper and sufficient care is taken for the maintenance of adequate accounting records, for safeguarding the assets of the company, and for preventing and detecting fraud. It is also under the obligation to ensure that the financial statements of the company reflect a ‘true and fair view’. This includes a mandate to disclose all frauds reported to the audit committee or the board of directors in its financial statements. Also, where there is a finding of fraud or other internal wrongdoing that renders the financial statements untrue, the board of directors can, once every year, file restated financial statements with the prior approval of the National Company Law Tribunal,2 providing details of the reasons for doing so. A restatement would, of course, not absolve the company or the concerned persons from liability as per the law.

Further, in relation to listed companies, the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015 (LODR), *inter alia*, impose disclosure requirements on listed companies with respect to events that may materially affect the price of their securities, which include instances of fraud by promoters, KMPs or employees. These must be reported in line with the disclosure requirements under the LODR.

Separately, the management of scheduled commercial banks and non-banking financial companies are under an obligation to mandatorily report instances of fraud to the Reserve Bank of India.

---

2 The government has notified the constitution of the National Company Law Tribunal (NCLT) and the National Company Law Appellate Tribunal (NCLAT) in terms of the Companies Act. Accordingly, the NCLT and the NCLAT have replaced the Company Law Board, which has been dissolved.
Currently, there is nothing stipulated in the law in terms of leniency towards companies (and their officers and KMPs) that voluntarily report fraud and other instances of wrongdoing to the authorities. Accordingly, any leniency that is extended by the authorities will be strictly discretionary and will depend entirely on the facts and circumstances of the particular case.

However, an exception to this principle is under competition law. Section 46 of the Competition Act read with the CCI (Lesser Penalty) Regulations 2009 (the Regulations) allow the CCI to impose a lesser penalty in cases where a whistle-blower has made full and true disclosure regarding a cartel. The CCI has discretion to grant a reduction in the penalty of up to 100 per cent if the applicant is the first to make a vital disclosure by submitting evidence of a cartel, enabling the CCI to form a prima facie opinion or establishing the contravention in a matter under investigation. The CCI also has discretion to grant a reduction in the penalty of up to 50 per cent to the ‘second in’ applicant and up to 30 per cent to a ‘third in’ applicant that makes a disclosure by submitting evidence that provides significant added value. The CCI, for the first time in 2017, issued an order granting leniency to a first applicant enterprise and the responsible individual therein, reducing their sentence by 75 per cent. The order has laid down the requisite considerations for the grant of leniency, including the issue of the timing of the disclosure and the question of value that the applicant added to the evidence available with the CCI at the commencement of the investigation.

ii Internal investigations

Internal investigations are not regulated by legislation and are determined in terms of internal policies and procedures that each company follows. It is typical for larger organisations to have policies that set out the manner of conducting internal investigations that may be triggered on account of, say, a whistle-blower complaint.

Internal investigations may take a variety of forms depending on the nature and gravity of the allegation and may encompass, for example, witness interviews, disclosure of documents, appointment of external experts, forensic support. Typically, it is not very common for employees to engage lawyers to represent them. Given the cloak of privilege that is granted to communications between an attorney and his or her client, appropriate waivers would be necessary from the employee to enable release and use of the privileged information in connection with the internal investigation.

However, regardless of the allegation, as a best practice, it is always prudent to ensure that any internal investigation follows the principles of natural justice. Further, a show-cause notice must be issued to the concerned employee, followed by proper fact-finding and then cross-examination by both management and the employee, to ring-fence the internal investigation from being challenged later as having been partial or vindictive. Last, detailed reports and logs of the entire investigation process should be maintained as evidence for future reference and copies of the detailed order or findings should be made available to the employee prior to levy of any punishment in order to keep the process transparent. Having said that, under the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act 2013, specified employers need to establish an internal complaints committee to provide redress for grievances pertaining to sexual harassment in the workplace.

Currently, there is no legal mandate to voluntarily share the results of an internal investigation with the government, subject always to the reporting and disclosure requirements in terms of the LODR (applicable to listed companies). Further, where a formal inquiry follows an internal investigation, it would be expected that all internal records and documents would be made available, subject to privileged communications.
Data privacy aspects of internal investigations have assumed paramount importance since the promulgation of the Information Technology Act 2000 (the IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the IT Rules). The IT Rules stipulate what constitutes sensitive personal data or information (these include sexual orientation, financial information, passwords, biometrics and medical records) and the manner in which the information is to be handled, the protection it must be accorded and circumstances where it may be released or transmitted to a third party. Extreme care must be taken to ensure that in the disclosure and processing of information in relation to an internal investigation, all sensitive and personal information is kept confidential and dealt with strictly in line with the legal mandate. Many companies engage independent third-party experts to assist with internal investigations. Once again, care must be taken to ensure that any sensitive or personal information is handled as per the IT Act and the IT Rules and appropriate prior permissions are sought before release or transfer of any sensitive or personal information.

The government has constituted a committee of experts under the chairmanship of former Supreme Court judge, Justice B N Srikrishna, to study various issues relating to data protection in India. The committee drafted a white paper and recommended a nuanced approach towards data protection, keeping in mind the delicate balance that needs to be struck to boost innovation while upholding the individual’s right to privacy. The committee sought public comments on the white paper through public consultation meetings and online submission of responses to queries raised in the white paper.

In light of the Supreme Court’s decision in Justice K S Puttaswamy (Retd) v. Union of India & Ors\(^3\) upholding the right to privacy as a fundamental right, and the white paper on the data protection framework for India, the government is set to overhaul the existing Indian data privacy and protection regime to bring it in line with international standards of data privacy and data protection. A proposed umbrella legislation is due to be rolled out soon in this regard.

Section 126 of the Evidence Act 1872 (the Evidence Act) renders any communication between attorneys and clients privileged and, accordingly, any communication, document or opinion given by them to the client cannot be disclosed to a third party unless there is specific consent by the client. This is, however, subject to certain exceptions, such as communication for any illegal purpose or the attorney coming to know that a fraud or crime has been committed by the client since the time that the attorney’s services have been availed of.

The privilege under Section 126 of the Evidence Act does not extend to in-house lawyers, since the primary legislation governing lawyers and advocates in India – the Advocates Act, 1961 – states that an advocate must be one who is enrolled with the bar council of a particular state and cannot be one who is in full-time employment. Further, judicial decisions have not been consistent on whether communications with lawyers in full-time employment would be subject to the privilege under Section 126 of the Evidence Act. Accordingly, if a company engages external counsel to represent it in an internal investigation, all communication in that respect would be considered to be privileged. However, if a company deputes its in-house lawyers to act on its behalf in an internal investigation, it is likely that such communication and any work product generated by in-house lawyers may not be deemed privileged.

\(^3\) Writ Petition (Civil) No. 494 of 2012.
iii Whistle-blowers

India has enacted the Whistleblowers Protection Act 2014 but this only provides for the protection of whistle-blowers who have reported the wrongdoings of public servants. However, with regard to private organisations, the Companies Act and the LODR have provisions that require companies to put in place a vigil or whistle-blower mechanism.

The Companies Act requires certain categories of companies (on the basis of turnover, paid-up share capital, exposure to bank loans, etc.) to have a vigil mechanism that is to be overseen and headed by the chairman of the audit committee (who must be an independent director) such that directors and employees can use the vigil mechanism to report genuine concerns in a manner as may be prescribed. The Companies Act also provides for safeguards against victimisation to be established in the mechanism itself, including access to the chairman of the audit committee in appropriate cases. Further, under the Companies Act, independent directors are required to ensure that there is an adequate and functional vigil mechanism and that the rights of any person using the mechanism are not prejudiced. They are also required to report concerns about unethical behaviour or fraud to the board of directors.

Listed companies must have a whistle-blower mechanism to enable stakeholders to report unethical practices. The details of the working of that mechanism (including access to the chairman, the manner of making a complaint and maintaining anonymity) must be reflected in a whistle-blower policy, which is to be made available on the company’s website.

In light of the above, while it is mandatory for companies to have a vigil mechanism, sufficient discretion is given to the company in relation to determining the manner of putting it into operation, subject only to the fact that the whistle-blower should not be victimised. Having said that, the law in this regard is still nascent and no other specific statutory safeguards are provided for. In view of this, investigations pursuant to a whistle-blower complaint would be carried out in line with the internal policies of the company subject only to principles of natural justice.

III ENFORCEMENT

i Corporate liability

Principles of corporate liability are statutorily enshrined and statutes also provide for vicarious liability for the relevant offence. Where there is a direct charge against KMPs or other officers, any individuals who are responsible for the culpable conduct of the corporate entity can also be convicted and jailed.

Judicial decisions of the Supreme Court have established that corporations can be prosecuted for criminal acts, including those requiring mens rea, just like individuals, and would be held criminally liable when an offence is committed in relation to the business of the corporation by a person whose control over the affairs of the corporation is so intense and pervasive that a corporation effectively thinks and acts through that person. However, the actions of a corporation cannot be automatically attributed to its KMPs, directors or officers unless it is factually established that such persons exercised control over the business affairs of the corporation so as to deem them the alter ego of the corporation. Notwithstanding the foregoing, corporate criminal liability is continuously evolving and developing in India.

4 Iridium India Telecom Ltd. v. Motorola, Inc. (2011) 1 SCC 74.
5 Sunil Mittal v. CBI (AIR 2015 SC 923).
In relation to defence of corporate conduct where attribution is at play, and the *inter se* interests of the company and the concerned individuals are antagonistic, it is advisable that the company and the individuals are not represented by the same counsel. Typically, it is advantageous to engage independent counsel when the interests are opposite; however, when the positions are aligned, common counsel is advisable.

### ii Penalties

The consequences of wrongful conduct by a company may have civil, administrative or criminal consequences. Civil liability and penalties include fines, blacklisting, debarment from future tenders, accessing capital markets, administrative encashment of bank guarantees and damages, and to the extent that such conduct has criminal implications, the corporation stands to face appropriate criminal indictment as well, including attachment of property under criminal law. Further, there have been instances of exemplary penalties, such as the cancellation of mining leases of coal mines (granted as far back as 1993) by the Supreme Court6 (Coal scam) and cancellation of 2G telecom licences by the Supreme Court7 (Spectrum scam), both on allegations of bribery and wrongdoing by businesses in connection with the granting of such licences.

The Companies Act prescribes both civil and criminal penalties for misconduct. Civil penalties include fines payable by the company or the officers of the company for offences such as non-maintenance of a register of members, default in holding meetings and non-payment of dividends. A criminal penalty entails imprisonment either of the director or the officer in default for not maintaining proper books of account, for not issuing proper prospectus or for fraudulent conduct of business, for instance. The government can also penalise erring government contractors by suspension or debarment of the business. The SFIO, a specialised investigative agency, was established under the Companies Act to investigate corporate fraud. It has the power to arrest and to carry out search and seizure operations.

The range of potential sanctions against companies do not vary according to the authorities bringing the sanction, but is determined by the law.

### iii Compliance programmes

Given corporate criminal liability, the question of defence assumes importance. Typically, Indian laws do not explicitly recognise compliance programmes as a defence *per se* to criminal charges or a mitigating factor. Traditional defences under criminal law do not offer sufficient guidance either. Investigations for corporate fraud are on the rise and to what extent compliance programmes would be considered a good defence is not clear at present. The Supreme Court may be called upon to settle the issue. However, a robust compliance programme certainly helps to delineate the roles and functions within a company and therefore has the effect of avoiding KMPs, who otherwise would not be directly responsible for the culpable conduct, from being needlessly dragged into an investigation.

Typically, for individuals who may be vicariously liable, due diligence, lack of knowledge and remoteness of role and responsibility are good defences. For corporate entities, robust outcome-oriented compliance programmes, including routine audits, timely detection and reporting, may be considered as a defence. In this regard, it may be pertinent to note that

---

6 Manohar Lal Sharma *v.* The Principal Secretary & Ors (2014) 9 SCC 614.
7 Centre for Public Interest Litigation and others *v.* Union of India and others (2012) 3 SCC 1.
in line with the UK Bribery Act 2010, the Prevention of Corruption Act 1988 (POCA), which is the primary Indian anti-corruption statute, may be amended to create a safe harbour and defence if the corporation is able to prove that it has put in place adequate procedures designed to prevent bribery and other offences punishable under the POCA.

The elements of a corporate compliance programme will vary depending on the risk assessments, taking into account factors such as the nature of the business, the countries in which it operates and the employee strength of the company. However, it is advisable that compliance programmes should have certain vital elements, for example a written code of compliance. The programme must apply to all the employees of the company, including senior management, and provide an anonymous hotline for complaints, whistle-blower protection, regular training and so on. There must be a periodic audit of the company operations to ensure that employees are complying with the programme.

iv Prosecution of individuals

In the event that only employees or officers of the corporation are being prosecuted, the question of managing employee relations is more a function of the peculiar facts of a particular case.

There is no prohibition on a company paying the legal fees of an employee who is being investigated or prosecuted. The relevant contractual arrangement with the employee will have a bearing on the decision of the employee's legal representation, engagement with lawyers or payment of legal fees. If the employee, for instance, is acting in the course of his or her employment, performing the duties prescribed and for benefit of the company, payment of legal fees would be an obligation and disciplinary action against the employee in this situation would seem unfair. On the other hand, if the conduct of the employee is egregious and outside the scope of his or her duty, determination of his or her contract would not be considered improper. Further, Indian companies typically purchase directors' and officers' liability insurance to insulate them from liability incurred during the course of their employment. The Companies Act specifically recognises this right and further, while under the old company law directors could not be indemnified by their company for breach of duty or negligence, there is no restriction under the Companies Act, especially where there is no fault on the part of the concerned director or KMP.

IV INTERNATIONAL

i Extraterritorial jurisdiction

Currently, the POCA deals with bribing of and the abetment of bribery of public officials in India and has an extraterritorial application towards all Indian citizens outside India. In other words, where an offence is committed by a citizen beyond the borders of India, the POCA will be applicable to that offence and be tried as such. Separately, the Foreign Exchange Management Act 1999 (and the subordinate legislation framed thereunder), which is the foremost exchange control regulation, applies to all offices, branches and agencies outside India owned or controlled by a person resident in India and to any contravention committed outside India. Further, the Competition Act empowers the CCI to enquire into any agreement or abuse of dominant position or combinations, anywhere outside India, to the extent that such acts are likely to have an appreciably adverse effect on competition in the relevant market in India, and pass such orders as it may deem fit. In furtherance of this, the Competition Act permits the CCI to enter into any arrangement with a foreign government.
India

Separately, India has ratified the United Nations Convention against Corruption and, in order to meet its obligations under the convention, the Prevention of Bribery of Foreign Public Officials and Officials of Public International Organizations Bill 2011 was introduced in Parliament. This was to deal with the bribery of and by foreign officials and officials of international organisations, penalising both. However, this Bill subsequently lapsed and no fresh Bill in this regard has yet been introduced in Parliament.

ii International cooperation

The extradition of a fugitive from India to a foreign country or vice versa is governed by the provisions of the Indian Extradition Act 1962 (the Extradition Act) and the basis of extradition could be a treaty between India and a foreign country. Under Section 3 of the Extradition Act, a notification must be issued by the government, extending the provisions of the Extradition Act to the country or countries notified. The Ministry of External Affairs is the central authority for all incoming and outgoing requests for extradition. India has currently signed extradition treaties with 37 countries and has extradition arrangements with eight others.

The Extradition Act specifies that any conduct of a person in India or in a foreign state that is mentioned in the list of extradition offences and is punishable with a minimum of one year's imprisonment qualifies for an extradition request. In the case of countries with which India does not have such a treaty, the central government can, by notified order, treat any convention to which India and the foreign country is a party as the extradition treaty providing for extradition, with respect to the offences specified in that convention.

India has also entered into mutual legal assistance treaties with 39 countries wherein both countries agree to exchange information to enforce criminal laws. Further, India is a party to the 1997 International Convention for the Suppression of Terrorist Bombings. This provides for extradition in terror crimes. Furthermore, India is one of the oldest members of Interpol and the CBI acts as the liaising agency with Interpol.

For matters and information pertaining to taxation, India is a party to a number of tax information exchange agreements with various countries (including several perceived tax havens such as the British Virgin Islands), which provide for transparent exchange of information between the countries in taxation matters. Finally, in matters of securities regulation, India is member of the International Organization of Securities Commissions and has signed the multilateral memorandum of understanding that represents a common understanding on the manner of consultation, cooperation and exchange of information for the purpose of regulatory enforcement regarding securities markets.

In terms of cross-border cooperation, the PMLA authorises central government to enter into an agreement with another government to permit the exchange of information for the prevention of an offence. Also, as noted above, the Competition Act empowers the CCI to enter into arrangements with foreign governments in connection with enquiries into acts outside India that have an appreciably adverse effect within the relevant markets in India. Similar powers are provided to the government under the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act 2015 for gathering information in relation to evasion or avoidance of tax or undisclosed foreign income.
iii Local law considerations

India has strict laws relating to data privacy and attorney-client privilege, as discussed above. Breach of any of these lead to stipulated punishments. Having said that, there are exceptions when the disclosure and release of sensitive or personal information may be permitted without the consent of the concerned person by an order under the law currently in force.

Indian law also recognises bank secrecy and there are a number of provisions in law that stipulate that transactions between a bank and its client shall be secret. Among these, the Bankers’ Book Evidence Act 1891 states that a banker cannot be compelled to produce the contents of its books and is permitted to maintain the secrecy of such transactions in a matter in which the bank has not been made a party. Such production can be forced only upon issuance of a court order from a judge with special cause. Under this legislation, the banks have a right to give notice of their intention to show cause against an order made by a court or a judge requiring disclosure.

Further, the Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act 1983 and the Banking (Regulation) Act 1949 contain provisions dealing with privacy principles and secrecy that must be accorded to the affairs of banks’ clients. The principles of banker-client secrecy are respected and upheld and only in exceptional circumstances can those principles be overridden and confidential information be permitted to be disclosed. Compliance with the law and public interest would be instances when disclosure would be deemed permissible. Having said that, an order by the appropriate government or a court would be necessary to effect the disclosure of confidential information overriding the statutory granting of secrecy and confidentiality of such information.

V YEAR IN REVIEW

India has witnessed a number of large scams during the past few years, which have brought issues of corporate governance, transparency and the role played by KMPs into the limelight. During the past year in particular, scams in the banking sector have brought to the forefront the malpractices that were being adopted by banks as a means of showing increased profits. One of these – the PNB-Nirav Modi scam – is considered to be one of the biggest corporate scams to date in India. In addition to the Alere Inc scam and CDM Smith declination, a number of other foreign companies have been investigated by the US Department of Justice for alleged violations of the US Foreign Corrupt Practices Act (FCPA). These investigations have been swiftly followed by other investigations and inquiries by Indian agencies, again underscoring transnational inter-agency cooperation.

i PNB–Nirav Modi fraud

This was a bank fraud to the tune of 144.5 billion rupees involving diamond merchants Nirav Modi and Mehul Choksi and their respective companies. On 29 January 2018, an official of the PNB from Mumbai filed a criminal complaint with the CBI against three companies and four people, including Nirav Modi and Mehul Choksi, the managing director of Gitanjali Gems Limited, alleging that they had defrauded the bank and caused a loss of US$43.8 million. It came to light subsequently that the company, in connivance with retired employees of PNB, got at least 150 letters of undertaking (LOUs) issued in their favour. The fake LOUs were recycled by the diamond jewellery group and illegally issued to other banks for borrowing money, allowing the Nirav Modi Group to defraud the bank and many other...
banks who gave loans to Nirav Modi. In addition to the 114.5 billion rupee PNB fraud, Modi also defrauded 17 other banks of 30 billion rupees. The matter is currently being heard by Indian courts.

ii Alere Inc

Alere committed various accounting violations, including the mischaracterising in its books and records of payments made to government officials by Alere Colombia and Alere India. Alere Colombia made payments of approximately US$275,000 during the course of several years to a management level employee at an entity involved in Colombia’s healthcare system, whereas Alere India paid its India distributor an increased commission intended for local government officials in order to increase sales of its products there by 400 per cent. Alere retained approximately US$150,000 in profits from the increased contracts even after new management discovered the commissions and ended the practice. On 28 September 2017, the SEC ordered Alere to cease and desist violations of the FCPA and other securities provisions, and further ordered the company to pay a civil penalty of US$9.2 million, disgorgement of US$3,328,689 and prejudgment interest of US$495,196.

iii Pilot programme declination – CDM Smith

On 29 June 2017, the Department of Justice (DOJ) reached a declination letter agreement with Boston-based engineering and construction firm CDM Smith Inc. According to the letter agreement, between 2011 and 2015, employees and agents of CDM Smith and its India subsidiary paid US$1.18 million to government officials at the National Highways Authority of India and to officials in Goa for a water project contract. CDM Smith voluntarily disclosed the payments to DOJ. As part of the declination letter agreement, CDM Smith agreed to disgorge just over US$4 million in profits from the tainted contracts and admitted to the DOJ’s brief statement of facts.

iv Sterling Biotech Limited scam

The ED arrested a former Andhra Bank director for his alleged role in the conspiracy by Gujarat-based Sterling Biotech Limited and others to cheat public sector banks of 53.83 billion rupees. The director was suspected of having received more than 15 million rupees from the Sterling Biotech group and is charged under the PMLA. The company's directors had obtained large-scale loans from Andhra Bank and others by showing falsified records of production, turnover and investments in capital assets. This was done by the company directors in connivance with the in-house chartered accountant of the company, who has also been charged with fraud.

v Deccan Chronicle Holdings Limited

A case under the PMLA was initiated against Deccan Chronicle Holdings Limited (DCHL), its management and others for causing wrongful loss of 3.577 billion rupees to Canara Bank. The CBI also registered five more First Information Reports in respect of loss caused to five public sector banks against DCHL, its management and others for causing wrongful loss of a total of 11.62 billion rupees to six public sector banks. An investigation conducted by the ED revealed that DCHL had obtained loans for working capital, the purchase of capital
goods and short-term loans by overstating the receivables, understating huge loan liabilities by furnishing fabricated financial statements and not disclosing the loans taken from other banks and non-banking financial companies.

VI CONCLUSIONS AND OUTLOOK

While India has a multitude of laws that seek to instil high levels of corporate governance and adequate safeguards in both the public and private sectors, it is the lack of enforcement and the general apathy of government authorities that has led to a significant rise in the incidence of scams during the past few years. While the number of scams involving government departments has reduced during the tenure of the current government, crimes in the private sector have continued unabated.

To counter and eliminate fraudulent collective-investment schemes designed to cheat members of the public, the government intends to introduce a new bill, the Banning of Unregulated Deposit Schemes and Protection of Depositors’ Interests Bill (the Bill), which will be based on Britain’s Financial Services Act 2012 and will provide for harsh penalties to deter companies and persons from implementing any collective investment schemes without obtaining due permissions. The Bill also proposes the creation of special courts in every state to handle cases of fraudulent deposit schemes. Should such a law be implemented, it may prove to be a deterrent for such crimes going forward.

Additionally, the SFIO, which comes under the Ministry of Corporate Affairs, is developing a new system for early detection of corporate fraud and to safeguard gullible investors from fly-by-night operators. The new system would also trawl social media platforms for leads on any possible fraud in the making. The SFIO floated a tender for selection of a managed service provider to develop this ‘early warning system’ (EWS). The idea of developing an EWS was first floated in 2009 after the Satyam fraud came to light. This new system would generate the data that helps to raise red flags and alerts using business intelligence and analytics capabilities. It would help with protecting investors from being exploited by deceitful companies or persons, and in identifying companies for further examination, scrutiny or detailed investigation by the Registrar of Companies, other offices within the Ministry of Corporate Affairs, or by the SFIO. The system would safeguard against disruption caused by incidents of corporate fraud, by proactively monitoring the operations of the companies through the statutory reporting mechanisms and other data that is in the public domain.

With Indian industry calling for adoption of hi-tech control systems to check financial frauds, some of the Indian banks have started deploying artificial intelligence, big data and blockchain technologies to better regulate their operations. The blockchain technology can be used to prevent scams like the one unearthed in Punjab National Bank. Blockchain technology allows entrepreneurs to incorporate their businesses into a digital distributed ledger, removing intermediaries in traditional processes and reducing friction. The Indian government has sounded an alarm likening cryptocurrencies to Ponzi schemes designed to dupe gullible investors. However, experts advise that the technology underlying such cryptocurrencies can be put to good use. The benefits of blockchain for users include those of data unmutability, verifiability, security and privacy. The PNB–Nirav Modi case (cited above) showcased an instance where PNB officials misused their access to PNB’s Society for Worldwide Interbank Financial Telecommunications (SWIFT) (the electronic messaging system) used for overseas funds transfers without registering the fraudulent transactions with
the bank’s internal transaction messaging system (the Core Banking Solution), enabling the fraud to remain undetected for a long time. While standard encryption is applied to messages sent via SWIFT, the system is not infallible and is vulnerable to hacking. The idea of using blockchain technology here would be to track every step of the process so that such actions do not remain undetected for long periods.

To conclude, while scams involving the government or their agencies appear to have reduced during the past couple of years, corruption in the private sector continues unabated. The current outlook suggests better enforcement of legislative provisions to curb instances of white-collar crime and more involvement by the government in ensuring a reduction of such crimes.
Ireland

Karen Reynolds, Claire McLoughlin and Nicola Dunleavy

I INTRODUCTION

In late 2017, the Irish government published a suite of measures aimed at strengthening Ireland’s response to corporate misconduct. During the next 12 to 18 months, significant changes may be made to the investigative and prosecutorial regimes that govern corporate Ireland.

In November last year, the Irish government published Measures to Enhance Ireland’s Corporate, Economic and Regulatory Framework. The focus of the framework is combating white-collar crime. The actions put in place by the government have been developed to augment the existing regulatory and legislative framework in the area of corporate, economic and regulatory crime. The planned measures serve as a further commitment by the government that Ireland is open for business and is a secure place in which to do business.

There are a number of bodies, regulatory and otherwise, which are empowered to investigate corporate conduct in Ireland including An Garda Síochána (the police), the Office of the Director of Corporate Enforcement (ODCE), the Office of the Revenue Commissioners (the Revenue Commissioners), the Competition and Consumer Protection Commission (CCPC), the Data Protection Commission (DPC), the Health and Safety Authority (HSA) and many other regulators. 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 Central Bank of Ireland (CBI) 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 investigation of criminal offences is primarily the function of the police. The police have a wide range of powers, which include: to approach any individuals and make reasonable enquiries to stop and search; to seize evidence; to enter and search premises; and 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

1 Karen Reynolds, Claire McLoughlin and Nicola Dunleav are partners at Matheson.
2 Measures to Enhance Ireland’s Corporate, Economic and Regulatory Framework, November 2017.
3 Ibid.
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.

The ODCE is afforded a wide range of investigative powers under the Companies Act 2014 and is responsible for 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, supervision of liquidators and receivers 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.4

The CBI is responsible for regulating the financial services industry. Its enforcement work can be divided into two processes: an administrative sanctions procedure by which the CBI 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 and of integrity, and financially sound. The CBI’s investigative powers include compelling the production of documents, compelling individuals to attend interviews and conducting on-site inspections.

The Revenue Commissioners is the government agency responsible for the assessment and collection of taxes. It also has investigative and prosecutorial powers, which include: to enter and search premises; to inspect goods and records; to take samples; to question individuals; to remove and retain records; to stop, search and detain vehicles; to seize and detain goods and conveyances; and to 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;5 to conduct investigations into trusts and offshore structures, funds and investments;6 and to obtain High Court orders.7 Of particular significance is the power to obtain information from financial institutions and procure search warrants to this effect.8

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 business.9 Its search powers are not confined to a company’s offices but extend to the homes of directors or employees.

The regulatory body previously known as the Office of the Data Protection Commission is now known as the Data Protection Commission (DPC) under the Data Protection Act 2018. It is responsible for upholding the rights of individuals and enforcing obligations upon data controllers under data protection law. If the DPC receives a complaint, it is obliged to investigate the alleged data protection breach. Additionally, the DPC may investigate the unlawful processing of personal data and audit data processors of its own accord. The

4 Section 949(c) and (d) of the Companies Act 2014.
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.
ODPC secures compliance with data protection law through the service of enforcement and prohibition notices on offending parties. It is an offence for any person who fails to, or refuses to comply with an enforcement notice without a reasonable excuse. 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 prosecution of corporate crime is not influenced by political agendas; the various investigative bodies are independent of government. Ireland is a low-risk economy and a secure place in which to do business.

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.

Businesses are under no obligation to cooperate with an investigating authority, save where provided for by legislation or in response to an appropriate court order. In all cases, businesses should seek legal advice regarding the extent to which they must cooperate and comply with the investigating authority. Voluntary compliance with a request for documents or information may affect the privilege against self-incrimination and any obligations of confidentiality under data protection laws.

II CONDUCT

i Self-reporting

There are a number of legislative provisions that impose a positive obligation on persons (including businesses) to report wrongdoings in certain circumstances:

a Section 19 of the Criminal Justice Act 2011 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. Practically speaking, 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.

b 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 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 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 Act. This obligation is notwithstanding any professional obligations of privilege or confidentiality on the part of the auditor.

Although in practice self-reporting may be a mitigating factor in prosecution, 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 Sanction 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’.  

The DPP has a general discretion whether or not 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. It is important to note that 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 business 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.¹¹

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 arises in communications between a lawyer and a client where there is no actual or potential litigation, but the client is seeking advice and not merely legal assistance. In *Miley v. Flood*,¹² 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 applies to communications between a lawyer and a client made in the context of contemplated or existing litigation. It is the broader form of legal professional privilege and also covers communications with third parties, such as experts.

Privilege over any document is a right of the client, which he or she may choose to waive. In general, the disclosure of a privileged document to a third party will waive privilege. Following the decision in *Fyffes v. DCC*,¹³ the courts will allow 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.

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 businesses have policies in place, they must review them to ensure they are aligned to the provisions of the Protected Disclosures Act.

---

¹¹ [2015] IEHC 809.
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 is prevented from 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 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:

- relating to the commission of an offence;
- non-compliance with a legal obligation (except one arising under the worker’s employment contract);
- a miscarriage of justice;
- endangerment of health and safety;
- damage to the environment;
- misuse of public funds;
- mismanagement by a public body; or
- 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 a rights commissioner of the Labour 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.\(^{14}\)

Although the motivation for making a disclosure is irrelevant, the protections as set out above are not available to those who deliberately make false disclosures as these are not considered to meet the test for having a reasonable belief that a wrongdoing has occurred. This provision aims to protect businesses 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.

### 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 (the Companies Act) 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 shall be guilty of an offence.

In contrast, Section 271 of the Companies Act provides that an officer of a company shall 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.

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 shall 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,\(^\text{15}\) albeit in the context of the imposition of civil liability on a corporation.

It is unlikely that companies and individuals could be represented by the same counsel, based on the rules governing conflicts of interest in the Solicitors’ Code of Conduct, which provides that:

> if a solicitor, acting with ordinary care, would give different advice to different clients about the same matter, there is a conflict of interest between the clients, and the solicitor should not act for both.

### 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\(^\text{16}\) (whereby the guilty party is required to pay compensation in respect

---


\(^{16}\) Section 6(1) of the Criminal Justice Act 1993.
of any personal injury or loss to any person resulting from the offence), adverse publicity orders17 (in the form of publication of the offence and the identity of the entity found guilty) and remedial orders18 (to undo the harm caused by the offence).

Another common sanction against businesses is a disqualification order. Under Section 839 of the Companies Act, 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, both monetary and administrative. 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.19 The CBI has used these powers to reach settlements with financial institutions for regulatory breaches; the size of these settlements has increased dramatically since the onset of the financial crisis in 2008. More recently, the monetary penalties imposed between 2015 and 2016 increased by nearly €5 million. This was particularly interesting given that the same number of administrative sanctions cases were concluded in both 2015 and 2016.20 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.

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.21 Furthermore, the Irish courts have jurisdiction under the Companies Act to disqualify an individual from acting as a director of a company if that individual is convicted of a competition offence on indictment.22

### iii Compliance programmes

Compliance programmes are not generally provided for in legislation as a defence to criminal proceedings. The Criminal Justice (Corruption Offences) Bill 2017 has now concluded the legislative process and was signed into law on 5 June 2018 as the Criminal Justice (Corruption Offences) Act 2018. The Act has not yet commenced; however, a commencement order is expected imminently. A notable provision, similar to the content of Section 7 of the UK Bribery Act 2010, is Section 18(2) of the Act. This contains an explicit defence for a

---

18 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.
19 The Central Bank (Supervision and Enforcement) Act 2013.
21 Section 2 of the Competition (Amendment) Act 2012.
22 Section 839 of the Companies Act 2014.
business that has committed an offence under the corruption legislation, if it can show that the business took ‘all reasonable steps and exercised all due diligence to avoid the commission of the offence’.

If a business 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 of a compliance programme may assist in reducing the quantum of any sentence to be imposed. However, any the programme should be effective in its implementation.

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.

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.

Additionally, the Companies Act largely restates earlier legislation, under which 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. 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. However, in practice, D&O policies tend to exclude losses resulting from fraud or dishonesty, malicious conduct and the obtaining of illegal profit.

26 Section 235(4) of the Companies Act 2014.
27 Ibid, Section 235.
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.*

Prosecutions of individuals under these provisions have been relatively rare in our experience.

**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 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 Criminal Justice (Corruption Offences) Act 2018 has now been enacted and is expected to be commenced imminently. The 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 read 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.

---

28 Section 8 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.
The fourth EU anti-money laundering Directive (AML IV) came into force on 25 June 2015 and has only been partially transposed into Irish law, to the extent that corporate entities are required to maintain registers of beneficial ownership. Many of the other provisions of the Directive are due to be transposed by the Criminal Justice (Money Laundering and Terrorist Financing) Amendment Bill 2018, which is due to be enacted by the end of 2018. The remaining provisions are expected to be transposed by way of statutory instruments. It imposes increased responsibility on ‘obliged entities’ (as defined under Article 2 AML IV) 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.

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.

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 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.

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. The transposition of the AML IV into Irish law will lead 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. It is expected that the Department of Finance will make a statutory instrument in the coming months, assigning separate legal responsibility to the Registrar of Companies for the maintenance of a central beneficial ownership register.

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.33

Under Section 4 of the Data Protection Acts, which are part of the comprehensive European data protection framework, data subjects have a right to access and to be supplied with all ‘personal data’ held by a data controller or processor. However, individuals may not obtain their personal data if the information is kept by a statutory body for the purposes of preventing, detecting or investigating offences.34

The General Data Protection Regulation 2016 (GDPR)35 recently became effective in each of the European Union (EU) Member States. The GDPR introduces significant changes to, among other elements, 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 the GDPR when offering services in the EU. The Law Enforcement Data Protection Directive 2016 (the 2016 Directive)36 was adopted in conjunction with the GDPR. The 2016 Directive governs the processing and exchange of personal information between law enforcement authorities in the context of criminal investigations. The Data Protection Act 2018 gives further effect to the GDPR and the 2016 Directive while largely repealing the current Data Protection Acts.

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, the right to a fair trial and the entitlement to fair procedures.

33 Tournier v. National Provincial and Union Bank (1924) 1 KB 461.
34 Section 5 of the Data Protection Acts.
V YEAR IN REVIEW

During 2017, the Charleton Tribunal, led by Mr Justice Peter Charleton, has been examining matters concerning protected disclosures made by members of the police.

The government signaled its intention to establish a new independent agency to greater enhance Ireland’s ability to undertake corporate law enforcement. The new agency will have more autonomy and flexibility to adapt to the challenges it faces in encouraging greater compliance with the Companies Act.

In recent months, the ODCE launched an investigation into Independent News and Media (INM) following a protected disclosure by INM’s former chief executive. During the course of this investigation, the ODCE uncovered details of a potential data breach and are in the process of making an application to the High Court to appoint inspectors to INM to investigate the affairs of the company.

The establishment of a police-led joint-agency task force on a pilot basis has also been proposed. It is envisaged that the task force will focus its activity on the issue of payment fraud.

As referenced, the Criminal Justice (Corruption Offences) Act 2018 has been enacted and is currently awaiting commencement. In a speech given in late 2017, the Minister for Justice and Equality, Charlie Flanagan TD, noted that ‘the reputation of a state and its business community can be affected by the rigour with which it tackles corruption . . . it is only by holding ourselves up to the highest standards, that we can tackle corruption effectively and maintain or improve the trust, respect and support of the Irish public’.

As mentioned, during the past year, we have also seen the enactment of the Data Protection Act, which, together with the entry into force of the GDPR in May 2018, amends data protection laws, creating a consistent data protection regime across the EU.37

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 recently signaled its intention 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.38 With that in mind, it seems likely that we will continue to see more enforcement across all regulated sectors in the future.

38 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, since 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 authorities2 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,3 with reference to insider trading and market-manipulation offences, and in close cooperation with the public prosecutor. Further,

---

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.
the latter is under an obligation to notify the president of CONSOB when a report of a
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.

4 Grande Stevens and Others v. Italy, 4 March 2014.
In such cases, prior to the initiation of trial proceedings, companies must:

\( a \) make good any damages in full;

\( b \) eliminate the harmful and dangerous consequences of the offence (or otherwise take efficacious 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,\(^5\) 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.\(^6\)

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 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 in the event that 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

\(^5\) 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.
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.

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 became aware on the basis of his employment relationship. The employee can not 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 has to 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 in the event that 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, in fact, 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:

a 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;

b at least one alternative signal channel that guarantees the privacy of the reporters;

c the prohibition of acts of retaliation or discrimination against the reporter for reasons connected, directly or indirectly, to the report; and

d 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.

---

7 Engel and others v. the Netherlands, 1976, and following cases, among which, Grande Stevens and Others v. Italy, 2014.
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, \textit{inter alia}:

\begin{itemize}
\item[a] public deeds or revenue stamps;
\item[b] criminal offences against individuals;
\item[c] criminal offences involving market abuse;
\item[d] bodily harm or manslaughter because of violations of health and safety regulations;
\item[e] receiving stolen goods;
\item[f] money laundering and the handling of illicit funds and assets;
\item[g] cybercrime;
\item[h] organised crime offences;
\item[i] offences against trade and industry;
\item[j] criminal offences against intellectual property;
\item[k] criminal offences against the environment;
\item[l] fraud against the state or a public body;
\item[m] corruption;
\item[n] forgery of money, tax stamps, credit cards and distinguishing marks of industrial products;
\item[o] corporate crimes;
\item[p] crimes of terrorism and of subversion of the democratic order;
\item[q] inducement not to make statements or to make false statements to the authority;
\item[r] employment of illegal immigrants;
\item[s] child grooming; and
\item[t] racism and xenophobia.
\end{itemize}

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 \textit{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, in order 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.

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 nor 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) a ban on carrying out business activities;

b) suspension of licences and concessions;

c) a ban on dealing with public bodies;

d) exclusion from or cancellation of public financing or contributions; and

e) a ban on advertising goods or services.

Publication of the conviction can be in one or more journals and include billposting 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.

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’.

---

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 (Trib. Milano,
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 prohibitory measures, or the suspension and subsequent conversion of the fines in the event that the reparatory action was carried out late.9

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 Confindustria10 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.

---

9 The Italian government nominated a review commission to empower the efficiency and the aim of prevention of Legislative Decree No. 231/2001.

10 Confindustria is an association representing manufacturing and service companies in Italy. Membership is voluntary.
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.

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 concerned11 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’12 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,13 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.14

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

---

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’s and five of its former and current managers of market manipulation charges relating to previous downgrades of the country’s sovereign debt.
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:

- offences against the state;
- offences of counterfeiting the state seal and use of the counterfeited seal;
- offences of forging money and public credit cards; and
- 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 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 behalf, performing the acts requested\(^{15}\) and transmitting their results to the requesting country. Alongside national legislation, such matters are governed by international conventions\(^ {16} \) (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.\(^ {17} \) Italian authorities refuse to allow extradition of defendants abroad:

- 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;
- for political offences; or
- in the event that the conduct in respect of which extradition has been requested is punishable by death in the requesting state.

Within the European Union, 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.

---

\(^{15}\) 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.

\(^{16}\) 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).

\(^{17}\) 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 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 seizable.

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:

- the collection of evidence;
- 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 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.
V 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 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) or the more recent case of market manipulation involving the insurance company Fonsai, 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 point of view, 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; 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. As an institution, the Bank of Italy has

---

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.
19 Both of which were judged by the Court of Cassation in 2012.
20 The Court of Turin rendered its judgment on October 2016.
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.
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.

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. Since this crime may be punished even if committed entirely abroad, an Italian public prosecutor could investigate market manipulation allegedly committed by rating agencies23 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. Other important banks are involved in criminal proceedings for the crime of bankruptcy: the Banca MB,24 Banca Etruria25 and Banca Carife (Cassa di Risparmio di Ferrara)26 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?

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.

23 As mentioned above, on 30 March 2017, the Court of Trani acquitted the ratings agency Standard & Poor’s and five of its former and current managers of market manipulation charges relating to previous downgrades of the country’s sovereign debt.

24 Ten former executives of the bank are on trial before the Court of Milan.

25 The former executive director of the bank and other former executives are currently under investigation from the office of the Public Prosecutor of Arezzo.

26 The executives of the bank are currently under investigation by the office of the Public Prosecutor of Ferrara.
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 American 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.

Chapter 17

JAPAN

Kakuji Mitani and Ryota Asakura

I INTRODUCTION

Under Japanese law, criminal sanctions are imposed on individuals, not on legal entities such as corporations. A corporation could be subject to criminal sanctions based upon certain ‘two-sided penalty provisions’, which stipulate that criminal penalties will be imposed on a company only if a person who belongs to the company commits a certain crime and that person’s conduct can be deemed the company’s illegal conduct. Criminal sanctions against corporations constitute economic sanctions such as fines, confiscation and the subsequent collection of money.

In addition to criminal sanctions, under Japanese law, various authorities may impose administrative sanctions, including cease and desist orders, surcharge orders and the imposition of heavy additional taxes. Thus, practically speaking, administrative sanctions have an important deterrent role against illegal misconduct by corporations. Administrative sanctions can potentially become quite large from an economic point of view.

Further, strong social criticism against companies involved in corporate wrongdoing may seriously impair an entity’s viability as a going concern. Thus, once a company gets involved in a scandal and it becomes public, the company must proceed with the necessary steps, including the internal investigation process, very cautiously.

Crimes related to corporate activities can be primarily categorised as follows:

a crimes to which the general Criminal Code applies – classic types of crimes such as embezzlement of company assets, breach of trust and fraud. The Criminal Code also applies to bribery and corruption;

b corporate crimes to which special provisions under the Companies Act apply – illegal dividend distribution, provisions of illegal benefits to shareholders, etc. The penalty for breach of trust in the case of directors under the Companies Act is stricter than typical cases under the Criminal Code;

c securities crimes under the Securities Law (the Financial Instruments and Exchange Act). In connection with certain accounting fraud cases, false statement on financial statements is often applied. In addition, insider trading is a crime under the Securities Law. The Securities Law also provides an administrative fine;

1 Kakuji Mitani is a partner and Ryota Asakura is an associate at Momo-o, Matsuo & Namba.
crimes to which other laws, such as the Antimonopoly Act (Competition Law) or tax laws apply (such as the Corporation Tax Act, the Local Tax Act and the Income Tax Act). The surcharge on illegal conduct or the penalty tax can often become a serious problem for companies from an economic or reputational perspective; and

business operations crimes, such as violations of environmental law, the Waste Disposal Law, the Food Sanitation Act and the Food Safety Act. In most cases, the sanction would be minor but a company needs to pay attention to the effect on its reputation.

The sole authority responsible for criminal procedures in Japan is the Public Prosecutor's Office (the Prosecutor's Office). Corporate crimes that many people pay attention to or controversial economic cases are handled by the Special Investigation Department, in which many prominent prosecutors are gathered and work with a great deal of drive and purpose. Other authorities conduct primary investigations in certain other specific areas. The Securities and Exchange Surveillance Committee handles securities crimes, the Japan Fair Trade Commission (JFTC) handles matters concerning the Antimonopoly Act, and the National Tax Service Agency conducts tax investigations under the relevant tax laws. These authorities may issue a cease and desist order, a surcharge order or administer a heavy tax through administrative procedures. If these authorities determine that a case is especially malicious, they may refer it to the Prosecutor's Office with the results of their own investigation. The Prosecutor's Office may prosecute the person who is involved and the company, as necessary.

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 Criminal Procedure Law. The National Police Agency has the same authority. Other authorities, such as the JFTC, have the authority to conduct an on-site inspection as part of an administrative investigation. In a legal sense, this inspection is basically a voluntary procedure and is different from the dawn raid process conducted by the Prosecutor's Office or the National Police Agency. However, the authorities are entitled to issue the submission order of relevant documents against a suspected company. Therefore, in a practical sense, the process is similar.

It is possible for a suspected company or person to contend its innocence. However, it may be difficult to prevent the authorities from obtaining materials that they believe are relevant to the case during a dawn raid or inspection process.

---

2 On-site inspections during administrative proceedings may be conducted by the Japan Fair Trade Commission (JFTC) (Article 47, No. 4 of the Antimonopoly Law), the Tax Office (Article 74-2 of the General Act of National Taxes) and the Financial Services Agency (Article 177(1) of the Securities Act).

3 Please note if a company uses a leniency programme for violations of the Antimonopoly Law, cooperation with the JFTC’s investigation is required, in principle.
Provisions of criminal sanctions regarding corporate activities are as follows:

<table>
<thead>
<tr>
<th>Relevant authority</th>
<th>Provisions of criminal sanctions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Prosecutor’s Office, National Police Agency</td>
<td>• General penal code offences (embezzlement, breach of trust, fraud, bribery, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Penal provision stipulated in the Companies Act (special breach of trust, illegal dividends, benefits, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Corruption offences such as the Political Funds Control Law, Public Offices Election Law</td>
</tr>
<tr>
<td></td>
<td>• Business-related laws such as waste disposal law</td>
</tr>
<tr>
<td></td>
<td>As a general rule, the Public Prosecutor’s Office and the National Police Agency are in charge of all punitive provisions under Japanese law.</td>
</tr>
<tr>
<td>Securities transactions monitoring committee, a division of the Financial Services Agency</td>
<td>• Penal provisions stipulated in the Securities Act of the Financial Instruments and Exchange Law (fraudulent statement of securities, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Insider trading</td>
</tr>
<tr>
<td>Japan Fair Trade Commission</td>
<td>Penal provisions stipulated in competition laws such as Antimonopoly Act, Sub-Contracting Act, etc.</td>
</tr>
<tr>
<td>National Tax Agency</td>
<td>Penal provisions stipulated in tax laws such as income tax law, corporate tax law</td>
</tr>
<tr>
<td>Japan Financial Intelligence Centre</td>
<td>Criminal profit transfer prevention law</td>
</tr>
<tr>
<td>Labour Standards Inspection Office</td>
<td>Penal provisions stipulated in the Labour Law, such as the Labour Standards Act</td>
</tr>
<tr>
<td>Consumer Affairs Agency</td>
<td>Penal provisions stipulated in consumer protection-related regulations, such as the Act on Specified Commercial Transactions and the Premiums Labelling Act</td>
</tr>
<tr>
<td>Financial Services Agency</td>
<td>Investment law, money-lending business law, etc.</td>
</tr>
</tbody>
</table>

II CONDUCT

i Self-reporting

If a company detects illegal corporate activities, the company may obtain certain advantageous treatment from the authority by voluntarily disclosing it. Below are some examples.

a The leniency programme under the Antimonopoly Law (Competition Law) and Sub-Contracting Act.

Regarding the violation of competition law, there is a legal leniency programme, under which if a company voluntarily declares to the JFTC a case of wrongdoing (i.e., a cartel or bid rigging) that may constitute a violation of competition law, an administrative fine on the company would be exempted or reduced. Specifically, of the first five companies that declare voluntarily after the JFTC investigation has begun, three companies can qualify for receiving surcharge reductions or exemptions. Prior to the commencement of the JFTC investigation, a company ranked first in the timeline of leniency applications would obtain a 100 per cent reduction and a company ranked second would obtain a 50 per cent reduction and so on. After the commencement of the JFTC investigation, the reduction percentage becomes smaller, but it is still possible to receive a 30 per cent reduction for a company ranking first.4

4 According to some news reports, in December 2017, Obayashi Corporation, one of the biggest general contractor companies in Japan, voluntarily declared its bid rigging regarding the construction of a new central bullet train (shinkansen). If the leniency programme is applied to Obayashi Corporation, it might be exempted from administrative fines of billions of yen. Subsequent to Obayashi Corporation, Shimizu Corporation, another of the largest general contractor companies, voluntarily declared its violation of competition law. It might be a case where not only the leniency programme in competition law is applied...
The Sub-Contracting Act, for which the JFTC has responsibility as well as the
competition law. The JFTC will not issue an administrative order to a company that
self-reports a law violation. There is no specific leniency programme stipulated in
current regulations.

Special laws that contain a legal leniency programme. The Law for Preventing
Unjustifiable Extra or Unexpected Benefit and Misleading Representation provides
that if a company voluntarily declares a violation to the Consumer Affairs Agency, it
can receive a 50 per cent reduction in fine.

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. It should be noted, in general, that 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.

A new framework for an immunity agreement between a criminal suspect and the
relevant authority has been adopted through an amendment to the Criminal Procedure
Code. The new law is effective from 1 June 2018. Under this new system, if a criminal
suspect provides the information used for another party’s criminal wrongdoings 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. However, voluntary
declaration of his or her wrongdoings only will not suffice as a requirement to provide
information about the criminal acts of others. In that regard, this system is different
from similar systems in other jurisdictions, such as a plea agreement in the United
States. See Section IV.

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
(whistle-blower systems) or through the provision of information by outside parties. In
recent years, many Japanese companies (typically auto-parts makers) have been implicated
in international cases, and the target companies have only become aware of legal action by
receiving a subpoena or other governmental notice from overseas authorities.

Internal investigations

As a recently adopted practice, when certain illegal activities are committed within a company,
the company sets up 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.

but also the new framework of the immunity agreement between a criminal suspect and the authority in
Criminal Procedure Code (see Section II.i, point e) is applied because a violation of competition law is also
criminal offence.
The members of the investigation committee vary according to the severity of the case 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 an external lawyer, or an expert, such as an accountant, as a member of the investigation committee. This is done to ensure objectivity and neutrality. The number of cases in which investigation committees include a third-party expert is increasing. In this context, 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.\(^5\) Although it is not compulsory to adhere to the JFBA guidelines, investigative committees established in response to instances of corporate misconduct are often established and operated in general accordance with the guidelines, and otherwise refer to or explain reasons why the guidelines are not being followed in a given situation. The contents of the guidelines mainly provide the activities that the third-party committee should perform (fact-finding investigation, analysis of causes and backgrounds, and generation of proposals on measures for prevention of recurrence) and the composition of members of a third-party committee (members should be truly independent and have no shared interests in the company under investigation).

In the case of a listed company, the Japan Exchange Regulation (JPX-R) issued the Principles for Responding to Corporate Scandals on 24 February 2016, in which third-party committees are required to be independent, neutral and professional. The JPX-R alleged there had been times when some listed companies did not properly respond to their wrongdoings.\(^6\) Under these circumstances, where the interest in wrongdoing is particularly pronounced, the results of an internal investigation are frequently publicly disclosed. In particular, if an internal investigation is conducted using a third-party committee, as described above, the investigation report, which sometimes comprises hundreds of pages, is published on the company’s website. As a result, 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 Corporation Law and Article 62(4) (6), (5) of the Companies Act). The contact for an internal reporting system often takes the form of a specific department within a company or a hotline to an outside counsel office (which may be a law office). 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 the protection for internal whistle-blowers, the Whistle-blowers Protection Act (enforced in April 2006) stipulates that an employee should not be dealt with disadvantageously

---

5 Updated on 17 December 2010.
6 See: https://www.jpx.co.jp/english/news/3030/b5b4p0000022z5j-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: https://www.jpx.co.jp/english/news/3030/b5b4p0000022z5j-att/preventive_20180330.pdf.
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 help a company set up an internal control system, the Consumer Affairs Agency (CAA) issued new Guidelines for Business Operators Regarding the Establishment, Maintenance and Operation of Internal Reporting Systems Based on the Whistle-blowers Protection Act of 9 December 2016.7

III ENFORCEMENT

i Criminal procedure

Investigation by the Prosecutor’s Office or the National Police Agency

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, since the number of public prosecutors in Japan is fairly limited, in the context of illegal corporate activities, its resources may rather be directed towards serious or socially controversial misconduct, such as corruption involving famous politicians, large embezzlement cases or breaches of trust implicating the public.

ii Administrative procedure

Investigation by the Securities and Exchange Surveillance Commission, JFTC, Tax Office and others

The administrative procedure that is conducted by authorities such as the Securities and Exchange Surveillance Commission (SESC), the JFTC, the Tax Office 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.

The aforementioned organisations have no authority to conduct a compulsory investigation. Therefore, all actions during an investigation should be processed voluntarily, in principle, on the premise of cooperation by the company. However, under many laws, any act preventing inspection by an authority itself constitutes a violation of law and is subject to criminal sanctions (indirect enforcement: the authorities have no power to conduct a compulsory investigation, but the company is effectively required to cooperate with the inspection). Thus, the investigative procedure by these authorities is enforced in a similar manner to the compulsory procedure, and companies typically follow and cooperate with the investigative procedure voluntarily, unless there are any special circumstances.

The administrative procedure can be divided into two categories: administrative investigation and investigation for criminal cases. Almost all cases will involve an administrative investigation, in which enforcement of the law is in the form of an administrative order or the imposition of a surcharge by the authority. In certain extreme cases, the procedure changes to an investigation for criminal cases, under which the authority collects evidence for future criminal cases and refers the case to the Prosecutor’s Office at the end of the procedure, unless the case cannot be established.

---

The administrative procedure and investigation for criminal cases differ in that, 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.  

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cases of violations related to Antimonopoly Act</td>
<td>180</td>
<td>275</td>
<td>150</td>
<td>128</td>
<td>138</td>
<td>149</td>
</tr>
<tr>
<td>Cases in which administrative orders were issued as a result of violations of Antimonopoly Act</td>
<td>22</td>
<td>20</td>
<td>18</td>
<td>10</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td>The aggregate amount of surcharge (billion ¥)</td>
<td>44,257</td>
<td>25,076</td>
<td>30,242</td>
<td>17,143</td>
<td>8,510</td>
<td>9,143</td>
</tr>
<tr>
<td>Cases of leniency applications (actually applied cases (only announced))</td>
<td>143 (9)</td>
<td>102 (19)</td>
<td>50 (12)</td>
<td>61 (4)</td>
<td>102 (7)</td>
<td>124 (9)</td>
</tr>
<tr>
<td>Cases of violations related to Sub-Contracting Act</td>
<td>18</td>
<td>16</td>
<td>10</td>
<td>7</td>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>Cases in which JFTC made administrative directions following violations of Sub-Contracting Act</td>
<td>4,326</td>
<td>4,550</td>
<td>4,945</td>
<td>5,461</td>
<td>5,980</td>
<td>6,302</td>
</tr>
</tbody>
</table>

With regard to violations of the Antimonopoly Act (Competition Law), the overall number of cases is decreasing, whereas the number of administrative directions under the Sub-Contracting Act is gradually increasing. The latter is a relatively minor violation from the perspective of the protection of sub-contractors, compared to other major corporate offences such as cartel or bid-rigging cases.

This decreasing trend is mainly because companies have become more aware of the risks of violating the Antimonopoly Act, not because enforcement by the JFTC has weakened. The JFTC is shifting its resources to enforcing violations of the Sub-Contracting Act.

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. Since 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. 

---


9 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.

However, some substantially equivalent rights to protect attorney–client communications are provided under Japanese law. The Criminal Procedure Code provides the right of refusal against confiscation, particularly based on the expert’s duty of confidentiality. 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’ procedure often seen in foreign 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 Act on Special Measures Concerning Civil Court Proceedings for the Collective Redress for Property Damage Incurred by Consumers (2013 No. 96) and claims are limited to those concerning consumer contracts.

IV INTERNATIONAL

i Basic framework under the Japanese Criminal Act

The Criminal Act 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 Criminal Act 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 (1980 No. 69) stipulates a framework of coordination with foreign authorities. In addition, there are a number of criminal assistance treaties as bilateral treaties.

The National Police Agency (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 2017, there were

11 Experts include an attorney, doctor, nurse, midwife and patent attorney.
1,815 Interpol requests for investigation assistance and cooperation from foreign countries to Japan, and 32 via diplomatic routes. The NPA requested assistance from foreign countries in 327 instances via Interpol and on 109 occasions through diplomatic channels.\(^\text{12}\)

### iii Extradition

The Act of Extradition (Act No. 68 of 21 July 1947) governs the relevant issues regarding extradition of a criminal offender to foreign countries. Japan has concluded the Criminal Extradition Treaty 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 (1) that the crime is committed in Japan or the United States and (2) 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 at the discretion of the Japanese government as to whether they 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 Criminal Procedure Code

In 2016, the Criminal Procedure Code was amended and the immunity agreement system was newly adopted (as stated in Section II.i, point 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 is 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;

\( c \) 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.

We cannot predict how this immunity agreement system will operate in Japan. In the future there is a possibility that voluntary declarations of company wrongdoing will increase through its usage.

ii Remarkable corporate crime cases

Olympus
On 27 April 2017, the Tokyo District Court ruled that the former management team of Olympus Corporation (Olympus) should be liable for damages of approximately ¥85.9 billion incurred by Olympus. This is a judgment on two lawsuits in which Olympus sued the former management team and launched a shareholder derivative suit against the same persons. This is not a criminal case, but ¥85.9 billion is an extremely large amount for a judgment in Japan. This means that it is now necessary for managers to keep in mind the potential for damages of such magnitude.

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.13

KOBELCO
In October 2017, Kobe Steel Ltd (KOBELCO), 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. KOBELCO’s materials were delivered to other major manufacturing companies, including Mitsubishi Heavy Industries, IHI and SUBARU. The chairman and the president of KOBELCO resigned from their positions in March 2018 to take responsibility for not detecting the problems.

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 and then develop into criminal prosecutions. More recently, companies are voluntarily establishing special committees to conduct internal investigations when a case comes to light.

Japan

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.
I INTRODUCTION

The Prosecutors’ Office has the power to investigate all kinds of criminal offences and has the sole power to prosecute an individual or entity (including corporations) to the court. 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 environment law violations, among others. 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 since lack of cooperation frequently triggers investigations that are longer in duration, and broader and more stringent in terms of scope.

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 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

---

1 Seong-Jin Choi and Tak-Kyun Hong are partners and Alex Kim is a foreign attorney at Shin & Kim.
2 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.
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. It should be noted that 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.3

In cartel investigations, there is a written leniency policy for self-reporting;4 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 self-reporter who meets the above requirements but has reported after the KFTC has initiated its investigation is still eligible for exemption of the administrative surcharge, and exemption from or mitigation of restraining orders.

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.5

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. There is no established practice regarding an employee’s retention of legal counsel during an internal investigation. It should be noted that Korea is not an ‘at will’ jurisdiction with regard to the termination of

---

3 ‘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).

4 Article 22.2 of the Monopoly Regulation and Fair Trade Act.

5 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).
employees. Therefore, even if an employee refuses to participate in an investigatory interview on the grounds that the interview will be conducted without the presence of the employee's lawyer, refusal alone would not necessarily constitute just cause for the termination of the employment agreement, unless refusal to participate would somehow constitute a material breach of that agreement.

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 recognised prior to the commencement of a criminal investigation or criminal proceedings. The issue at hand was whether a memorandum containing incriminating information and written by the attorney of the defendant was inadmissible due to attorney–client privilege. The Supreme Court’s rationale appears to have been that the need to protect attorney–client communications is reduced when there are no criminal proceedings against the client. It is not clear whether the Supreme Court recognises 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 (1) 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 (2) to remain silent before the court on matters regarding confidential information. It should be noted that 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 incidents in which the FSS has requested financial institutions to submit memoranda written by external counsel or emails between the financial institution and its external counsel when that information was in the financial institution’s custody.

### 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.

---

6 Supreme Court of Korea, judgment 2009DO6788, 17 May 2012.
7 Article 317 of the Criminal Act.
8 Article 112 of the Criminal Procedure Act.
9 Article 149 of the Criminal Procedure Act.
10 Young-Ik Choi, ‘What if FSS requests submission of memorandum written by lawyer?’, *Law Times*, 20 January 2015.
11 Articles 13, 15 and 26 of the Protection of Public Interest Reporters Act (PPA).
The PPA sets forth the following elements with regard to whistle-blower incentive programmes:

a. retaliation against or interference with whistle-blowing is prohibited; 13
b. when serious harm to the life or body of a whistle-blower is expected, police protection may be provided; 14
c. 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; 15
d. 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; 16
e. 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; 17
f. 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; 18

g. if a whistle-blower suffers a loss (e.g., decrease in wage or additional expenses arising from the transfer of his or her job), upon filing from the whistle-blower, the government can provide relief funds to the whistle-blower and then later subrogate the whistle-blower’s claim against any third party; 19

h. the personal information of the whistle-blower may be treated on a no-name basis during the investigation and relevant proceedings, 20 and should not be disclosed to any third party without prior consent from the whistle-blower; 21 and

i. if the incentives provided under other bodies of legislation are more beneficial to the whistle-blower than the aforementioned incentives set forth in the PPA, the more favourable incentives set forth in other bodies of legislation shall prevail. 22

III  ENFORCEMENT

i. Corporate liability

Although the Criminal Act, which governs traditional crimes such as bribery, embezzlement or fraud, does not recognise corporate criminal liability, various other statutes imposing industry-specific or subject-specific regulations (e.g., those on securities, construction,

13 Article 15 of the PPA.
14 Article 13 of the PPA.
15 Article 14 of the PPA.
16 Article 26 of the PPA.
17 Article 14 of the PPA.
18 Id.
19 Article 27 of the PPA.
20 Article 11 of the PPA.
21 Article 12 of the PPA.
22 Id. The current ceiling of compensation under the PPA is 2 billion won, but the ceiling for reporting competition law violation or tax law violation is 3 billion won (Article 3 of Guideline for Compensation of Persons Who Report Competition Law Violation; Article 84-2(1) of the Framework Act on National Taxes).
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:

*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.*

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:

- a. the scope of the corporation's business;
- b. the title and position of the employee in question;
- c. the relevance between the illegal act committed by the employee and the business of the corporation;
- d. the motive behind the illegal act and follow-up action;
- e. whether the corporation knew of the commission of the conduct or was involved therein, and if so, to what degree; and
- f. the source of the money used by the employee in carrying out the conduct, and to whom the profit therefrom is attributed.23

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.24

With respect to civil liability, the principle of *respondeat superior* applies.25 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.26

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.27 There is not a significant volume of court precedent on this issue, but it is not uncommon, at least during

---

23 Supreme Court of Korea, judgment 96DO2699, 14 February 1997.
24 Supreme Court of Korea, judgment 93DO344, 14 May 1993.
25 Article 756 of Civil Act (Employer’s Liability for Compensation): (1) a person who employs another to perform a specific affair is liable for compensating for any loss inflicted on a third person by the employee in the course of performing the specific affair: provided that this shall not apply where the employer has exercised due care in appointing the employee and in supervising the performance of the specific affair, or where the loss has been inflicted even if the employer has exercised due care; (2) a person who supervises the performance of a specific affair on behalf of the employer shall also assume the same liability as prescribed in paragraph (1); and (3) in cases falling under situations (1) and (2), the employer or the supervisor may claim for reimbursement from the employee.
26 Supreme Court of Korea, judgment 97DA58538, 15 May 1998.
27 Article 22 of the Ethical Code of the Korean Bar Association.
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. An object used in a crime, produced or acquired by the criminal conduct, or acquired in exchange for the object above, can be confiscated. If confiscation is impossible, the equivalent monetary value should be collected.\(^{28}\) 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;\(^{29}\) the ceiling for the debarment period is two years.\(^{30}\) 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.\(^{31}\) 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 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.

\(^{28}\) Article 48 of the Criminal Act.

\(^{29}\) Article 27 of the Act on Contracts to Which the State is a Party.

\(^{30}\) Article 27(1) of the Act on Contracts to Which the State is a Party.

\(^{31}\) In 2016, the number of cases in which the KFTC imposed an administrative surcharge was 111 and the total amount of surcharges imposed by KFTC was 803.8 billion won (a simple calculation shows that 7.24 billion won was imposed per case). In 2015, the number of cases was 202 and the total of surcharges was 588.9 billion won. Press Release, KFTC, 10 May 2017. (www.ftc.go.kr/news/policy/competeView.jsp?news_no=3318&news_div_cd=1).
Although courts have yet to establish clear standards on the specific measures and actions that should be taken by corporations in order 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:

- the intent and purpose of the law that the corporation is being charged with violating;
- the degree of infringement of said law;
- the intent of the legislator in imposing corporate criminal liability with regard to the violation in question;
- the details of the violation and the degree of damages or consequences caused thereby;
- the size of the corporation and the feasibility of supervising individuals who commit violations; and
- the measures or actions taken by the corporation to ensure the prevention of such violations.32

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.33 In this regard, a corporation should:

- periodically update its internal compliance manuals;
- provide regular training sessions for employees;
- evaluate factors that cause corruption and analyse the business activities of each department to understand risks and conduct and tailor proportionate supervision accordingly;
- establish an internal control and compliance system;34 and
- conduct a thorough internal investigation and establish a policy of zero tolerance when any violation is detected.

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.35

---

32 Supreme Court of Korea, judgment 2009DO5516, 14 July 2011.
33 Supreme Court of Korea, judgment 92DO1395, 18 August 1992.
34 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 anti-corruption information management programmes or a comprehensive system linked to existing accounting, reporting or training system.
35 In a case where a business allowed a minor in its video-watching room (which are adult-only facilities in 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.
iv Prosecution of individuals
Since 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 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. 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.

IV INTERNATIONAL
i Extraterritorial jurisdiction
Generally, Korean authorities have no jurisdiction over conduct that occurs outside the Korean territory or is committed by a foreign national or a foreign company unless Korea or Korean citizens are affected by such conduct. Likewise, the authorities do not spend significant resources concerning the conduct of companies outside Korea, whether foreign or domestic, unless the conduct has a substantial effect on Korea or its citizens.

ii International cooperation
The 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

36 Supreme Court of Korea, judgment 2007DO9679, 26 June 2008; Supreme Court of Korea, judgment 2005DO9861, 8 September 2006.
in each country). Although Korea has extradition treaties and mutual legal assistance treaties (MLATs) with major countries, in practice extradition is permitted in only a small number of major cases. Between 2004 and 2015, Korea requested the extradition of 18 persons and received extradition requests for seven persons on average each year. For the same period, Korea requested MLATs for 81 cases and received MLATs for 70 cases annually. The average number of suspects repatriated into Korea between 2011 and 2015 was 131 annually.

iii  Local law considerations

Since 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 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, and depends on whether it is a routine investigation or a special investigation. 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. Whether note-taking by an attorney during investigations is permitted also differs between agencies and investigators. Investigators often keep asking questions even after the defendant opts to remain silent. When authorities interview a witness (i.e., a person who is not a suspect or a defendant), the witness is not allowed to receive the assistance of counsel 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.

40 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.
41 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.
42 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).
43 The police have internal rules that, in principle, allow witnesses to have the assistance of counsel during an interview. Article 11 of the Rules on the Assistance of and Interview with Counsel (National Police Agency Order, No. 702, 19 April 2013).
V YEAR IN REVIEW

A very stringent and thorough new anti-corruption law, the Improper Solicitation and Graft Act, was introduced in September 2016. The new Act 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, it 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, 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, provision of that benefit is punished by a surcharge regardless of whether it is provided to receive an improper advantage.44

Between late 2016 and mid-2018, the corruption investigations and trials involving former President Park, her confidant Choi and a couple of Korean conglomerates were the most influential cases in Korea. In April 2018, Seoul Central District Court rendered a judgment imposing 24 years’ imprisonment and a fine of 18 billion won to former president Park for bribery, abuse of power, coercion and divulgence of official secrets.

VI CONCLUSIONS AND OUTLOOK

From a global perspective, government investigations in 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 improvement with respect to the protection of an individual’s or a corporation’s procedural rights during an investigation, including by broadening the scope of attorney’s assistance during interrogation and recognition of attorney–client privilege and the doctrine of attorney work-product privilege. Although international cooperation is growing, there is still the practical obstacle posed by a lack of resources and language barriers. The corruption case surrounding former President Park shows that there is room for growth with regard to prevention of corruption in Korea, and it is possible that former President Park’s case may trigger additional legislation or enforcement with regard to anti-corruption efforts.

44 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 wreathes 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.
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 to 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 at every instance in which 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.

At the beginning of 2016, the structure of prosecutors’ offices underwent key reforms. 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 are to 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 obligated 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 tasks carried out in a specific case.

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

---

1 Tomasz Konopka is a partner at Sołtysiński Kawecki & Slezak.
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. During the course of an investigation, a law enforcement body may request that a business entity voluntarily provides documents that could represent evidence in a case. If 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 financial penalty 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 suspicion of a crime constitutes a separate criminal offence and the perpetrator is subject to the 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.

With respect to fiscal crimes, it is only possible for the person responsible for committing the act to avoid criminal fiscal liability by making an ‘unprompted 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 responsibility 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.

Parliament is currently working on the Bill on Transparency in Public Life (which may enter into force before the end of 2018). The draft Bill provides for several examples of self-reporting obligations on many entities, especially those in the finance sector or entities in which the State Treasury has shares. One of the many new obligations is a duty to publicly disclose details of contractual relations with other contracting parties, if the value of the contract exceeds 2,000 zlotys.

**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 not only conducted 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 (such as banks or investment firms) are obligated 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.

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 due to the operation in Poland of companies regulated by the strict rules of the US Foreign Corrupt Practices Act or the UK Bribery Act.

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 General Data Protection Regulation).
Processing of personal data (except sensitive data) is generally permitted within an internal investigation. However, it is recommended to obtain the necessary consent from the person to whom the data relates.

The above-mentioned draft Bill on Transparency in Public Life also provides for an obligation to introduce internal anti-corruption procedures. This duty is addressed to at least medium-sized entrepreneurs and public sector entities as a countermeasure to bribery offences described in Polish Penal Code. Failure to fulfil such a duty is an offence punishable by a fine of between 10,000 and 10 million zlotys.

iii Whistle-blowers

As it stands, Polish law does not impose sufficient regulation on whistle-blowing. However, employees who disclose irregularities or other undesirable circumstances within an organisation do 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 draft Bill contains regulations for protecting whistle-blowers. Namely, if the status of whistle-blower is granted by the prosecution, that person's employment contract cannot be terminated or changed to less favourable terms without the prosecutor's permission.

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 never been significant.

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 new, 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.

As of 1 May 2017, banks in Poland are obligated 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.
III ENFORCEMENT

i Corporate liability

The 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
- administrative 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.

Liability on the basis of the above-mentioned Act may be imposed in the event that one of the following is proven: at least a lack of due diligence in the choice of the person representing the entity, who is at the same time the perpetrator of a crime, or the defective organisation of the company, which did not ensure the avoidance of the commission of the crime, and this would not have occurred had due diligence been observed in its organisation. Note that 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 of such transformations at a company to prevent it from avoiding liability.

It should be emphasised that it follows from practice to date that the law enforcement bodies do not commence proceedings in every case in which such a possibility arises. 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
obligated 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 and 5 million zlotys (but which 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 form 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 from 560 zlotys to more than 16 million 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

Now 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. Note, however, that the draft Bill foresees such an obligation being introduced.

In reality, the existence of a compliance programme and ensuring its existence may significantly limit the risk of liability under the Act on Liability of Collective Entities for Acts Prohibited under Penalty, even if the commission of a crime resulted from inappropriate organisation.

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, newly amended 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, 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 a written
termination of the employment contract, and these reasons can be verified by the court if the
employee appeals to the Labour Court. In the event that 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.
The Ministry of Justice is working on amendments to the Act on Liability of Collective Entities for Acts Prohibited under Penalty; however, the amendment Bill has not been announced yet. From press reports and statements by ministry officials, it follows that the previous requirement of final conviction of a natural person as a condition of the collective entity’s responsibility will be eliminated. Among the expected changes are removal of the list of crimes for which a collective entity could be held responsible. This means that the responsibility of a collective entity will not be restricted to the prohibited acts indicated by the legislator, but the list of crimes will be open. The amount of the fine will be raised to between 30,000 zlotys and 30 million zlotys. Moreover, a collective entity will have to implement compliance procedures to run a company not only in accordance with the law, but also in accordance with ethical standards, risk management rules and other internal standards. The planned date of entry into force of these amendments is not yet known.

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 obligated 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 an 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) 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 excluded in principle. By way of 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.
Poland

Poland enforcement authorities routinely cooperate with 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 VAT fraud and other kinds of business crime. One of the amendments to the Criminal Code introduced more severe treatment for producing or handling fake or otherwise unsound invoices, which usually constitute one element of a wider VAT fraud. The government prepared an amendment, which introduces a ‘split payment’ system to separate net payments from VAT payments in business-to-business transactions. The president signed an amendment, which will come into force on 1 July 2018. The government is also planning to introduce an automated system of data-collection scanning and aggregating information about bank accounts. This system will also automatically assess the risk of a given undertaking being involved in tax fraud, money laundering and other business crime.

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.

Under the newly introduced Articles 270a and 277a of the Criminal Code, forgery of or tampering with an invoice in relation to circumstances influencing the amount of tax (or other public obligation) or its refund, in order to use that invoice as an authentic one, or using a fake invoice constitutes a separate offence. The perpetrator is liable to imprisonment for between six months and eight years. If the perpetrator forged or used invoices documenting transactions of which the value exceeds 10 million zlotys or made forgeries or used fake invoices as a source of their permanent income, the offence is considered to be a felony. A perpetrator in this case is liable to imprisonment for between five and 25 years.

Under the Act of 23 March 2017 on the amendment of the Criminal Code and certain other acts, there is a new institution in criminal law called ‘extended confiscation’. According to this regulation, all the assets acquired by the perpetrator during the five years prior to committing an offence would be considered a benefit thereof, unless the perpetrator or the other interested party can submit evidence in rebuttal. This applies in the case of sentencing for:

- an offence resulting in direct or indirect benefit of a substantial value;
- an offence subject to a penalty of five years or more than five years’ imprisonment resulting in – even potential – direct or indirect benefit; or
- an offence committed in an organised criminal group.

The Act on Trading in Financial Instruments and certain other acts have been amended to bring the Polish legal system in line with EU market abuse regulations, which significantly
altered national regulation of securities frauds, insider trading and other offences related to financial instruments and public companies. An entirely new institutional framework was implemented, effective from 1 January 2017, to detect tax fraud and process internal revenue matters, namely the National Tax Administration. The new framework resembles the old one in some respects but is much more integrated and centralised, which is supposed to improve its efficiency. Additionally, the simultaneously amended regulatory framework of tax proceedings was designed to hamper tax optimisation and refuse more requests for individual interpretations of tax law, which, in practice, reduced the clarity and integrity of the tax law.

The new Act on Counteracting Money Laundering and Financing Terrorism was enacted on 1 March 2018 and will enter into force later this year. The purpose of this Act is to increase the effectiveness of the national system of counteracting money laundering and the financing of terrorism. The main changes concern the creation of the Central Registry of Real Beneficiaries and the establishment of the Financial Security Committee. Moreover, the Act introduces new rules for interrupting transactions and blocking accounts. It also expands the list of institutions obliged to report on specific transactions and defines mechanisms for preparing a national assessment of the risks associated with money laundering and financing terrorism. Included in the definition of 'obligated institutions' are attorneys-at-law and legal advisers providing specified services to clients, such as the purchase or sale of real estate, enterprise, cash management of clients, making contributions to a capital company or increasing share capital of companies. Obligated institutions will have a duty to apply financial security measures to their clients, which are designed to recognise the risk of money laundering and financing terrorism and, if necessary, to keep the documentation. Financial security measures include customer identification, verification of identity or assessment of economic relations, and will be use, for example, when establishing business relationships or making an occasional transaction equivalent to €15,000 (if it seems to be related, it does not matter if it is one or several), which includes a transfer of money in excess of the equivalent of €1,000.

VI CONCLUSIONS AND OUTLOOK

The government is still doing extensive work on the Bill on Transparency in Public Act, which aims to increase social control over people exercising public functions. It is expected to enter into force later in 2018. The most important provisions are the obligation to introduce internal anti-corruption procedures, granting a special status of whistle-blower for people who give reliable information about corruption offences, and records of civil law agreements are kept by public finance sector entities.

The general outlook is that the government is ready to ensure better crime detection as well as the sure and harsh punishment of criminals. The National Prosecutor has issued new instructions on the scale of penalties demanded in the case of economic crimes. Investigators should demand not less than 10 years' imprisonment for damages that exceed 10 million zlotys in value, seven years for damages exceeding 5 million zlotys, five years for more than 1 million zlotys and three years if damages exceed 200,000 zlotys.

After the reimposition of the 'inquisitive' model of proceedings, prosecution offices seem to be working more effectively, especially given the reduced scope of assigned tasks. However, the recent restructuring of the entire prosecution system is the subject of serious doubts.
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 will take action against anticompetitive agreements, abuse of dominant positions, and mergers and acquisitions that substantially lessen competition. The CCCS has the power to require the production

---

1 Jason Chan, Vincent Leow and Daren Shiau are partners at Allen & Gledhill.
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.

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.

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 in order 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 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 co-operators 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.

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. 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 in order 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

Generally speaking, corporate conduct as a whole is punishable. That said, as a legal entity, a company necessarily acts through its officers and servants. Hence, insofar as criminal liability is a concern, any corporate wrongdoing is likely to also involve the acts of particular individuals. These particular individuals may, apart from the company’s liability, be themselves guilty of an offence or be subject to civil liability. There is no bar against criminal liability being imposed on both the company and its officers and employees, or civil liability being imposed on both the company and its officers and employees (subject to the principle of double recoverability).

Criminal liability

A company can be subject to criminal liability for the conduct of its officers and employees. Under Singapore law, a ‘person’ is defined as including body corporates unless the contrary intention appears. Hence, insofar as a criminal statute purports to impose criminal liability on any person, a company can accordingly be held directly liable unless the criminal statute intends otherwise. This depends on the wording of the criminal statute in question. As a legal entity, a company necessarily acts through its officers and servants. Thus, a company may 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 (i.e., an offence that does not require the prosecution to prove the existence of a guilty mind, such as intention, recklessness or knowledge). If a company’s employees have caused the commission of a strict liability offence, the company may be held liable.

Second, a company may also be guilty of an offence that requires the existence of a guilty mind. However, since a company, as a legal entity, has no physical existence and cannot have a ‘mind’ of its own, the law imposes liability in such cases by attributing the actions and intentions of the relevant natural persons to the company. Under Singapore law, criminal liability of a company may accordingly arise where an offence is committed during the course of the company’s business by a person in control of its affairs to such a degree that his or her actions and intent are the actions and intent of the corporation – this person must be found to be the ‘directing mind and will’ of the company. It is a question of mixed fact and law whether a person is to be found the ‘directing mind and will’ of the company. Typically, persons who may be held to be as such will include ‘the board of directors, the managing director and perhaps in some cases other superior officers of [the] company [who] carry out the functions of management and speak and act as the company’.

Third, a company may be subject to civil liability for the conduct of its officers and employees. A company may, in addition to its own personal liability for wrongdoing, be liable for the tortious acts of its servants committed during the course of their employment under the doctrine of vicarious liability.

Civil liability

A company can also be subject to civil liability for the conduct of its officers and employees. A company may, in addition to its own personal liability for wrongdoing, be liable for the tortious acts of its servants committed during the course of their employment under the doctrine of vicarious liability.
Generally speaking, corporate conduct as a whole is punishable. That said, insofar as criminal liability is concerned, any corporate wrongdoing is likely to also involve the acts of particular individuals. These particular individuals may, apart from the company's liability, be guilty of an offence themselves. There is no bar against criminal liability being imposed on both the company and its officers and employees.

**Legal representation**

There is generally no objection to a company and its employees being represented by the same counsel in the same matter where their interests are aligned. However, if in a particular case there arises a conflict or a risk of conflict between the interests of the company and the interests of the employee in respect of the matter, it is typically preferable that separate representation be sought as this would avoid the situation of the counsel having to discharge him or herself from acting for both the company and the employees.

**ii Penalties**

The penalties that can be imposed depend on the nature of the liability (criminal or civil) and the specific statute in question.

If a company is convicted of a criminal offence, the sanction is typically the imposition of a fine. However, depending on the offence in question, the courts may also impose additional sanctions, including a compensation order.

The SFA further provides that the MAS may, in relation to certain prescribed offences under the SFA, bring an action in the courts (in lieu of prosecution) for an order for a civil penalty in respect of that offence. A civil penalty made by the courts under that statute will be payable to the MAS. If this is not paid, the MAS may enforce it as though it was a judgment debt due to it. Claimants who have suffered loss may also have a right to recover compensation.

Insofar as a business is a holder of regulatory licences, these licences may be subject to conditions or the authorising statutes under which they are issued may provide for their revocation in the event of contravention of those conditions or of a particular written law. The power to revoke a licence is usually a regulatory power that may not be contingent on a judicial finding of wrongdoing.

Finally, there may also be consequential penalties that flow from a conviction (or even in the absence of a conviction depending on the nature of the misconduct). For example, if the company in question is listed on the SGX-ST, the SGX is empowered under the Listing Manual to impose sanctions on the company, such as a private warning, public reprimand, suspension of the trading of its securities, or even a delisting of the company.

**iii Compliance programmes**

Unless specifically provided for under a particular statute, the existence of a compliance programme does not function as a legal defence to the commission of a criminal offence. That said, companies should, nevertheless, have in place reasonable compliance programmes. What is a reasonable compliance programme depends on the risk in question that it is intended to address and the costs involved and there is no hard and fast rule as to what any particular programme ought to prescribe. The existence of compliance programmes may also lower the risk of breaches or the duration of any breaches (which may affect the penalty that may be imposed on the company).
The existence of a compliance programme may also be relevant at one of two stages insofar as criminal charges levied or contemplated to be levied on the company are concerned. First, the existence of a compliance programme may be a relevant factor that a prosecutor takes into account in the exercise of their discretion whether to prosecute or continue to prosecute a company in respect of which a criminal offence has been disclosed. Second, the existence of a compliance programme may also be relevant as a mitigating factor after the conviction of the company insofar as the appropriate sentence or penalty to be imposed on the company is concerned.

Note also that a compliance programme may assist the officers insofar as their liability is concerned in that it may allow them to show that the offence in question 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 against the authorities seeking to hold a particular individual liable under criminal law as well, whether in addition to liability on the part of the company or otherwise. If an officer of a company, especially a senior officer, is accused of corporate wrongdoing, this will inescapably have reputational effects on the company, regardless of whether the company itself is also charged. How the company manages the continued relations with the individual in question should, therefore, be guided with such considerations in mind.

There is no obligation on the part of the company to dismiss or discipline an individual who has been the subject of a criminal investigation or charged with a criminal offence. That said, this is dependent on the company’s internal policies and the view that the company takes with respect to the individual’s conduct. For example, 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 (generally contained in an employment handbook that has been incorporated into the employment contract by reference). Where, for example, the evidence that is known to the company suggests there are grounds for taking disciplinary action or for terminating an employee’s employment, the company may do so regardless of the outcome of the criminal investigation or prosecution against the employee.

Needless to say, the company should cooperate with the investigators insofar as they are legally obliged to do so. For example, the authorities may require that the 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, for example, 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. It is also 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 laws have been enacted by Parliament to extend the reach of particular statutes 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 legislation, also contemplates extraterritorial application, providing at Section 34 that certain offences thereunder if committed outside Singapore would be deemed to be committed in Singapore and that the person in question may be charged, tried and punished accordingly, and, further, that if a Singapore citizen commits certain other offences outside Singapore, they may be dealt with as though they were committed in Singapore.

Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act

Finally, the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA), which is the principal statute criminalising money laundering, also contemplates extraterritorial application. This is clear from Section 3(3) and (5) of the CDSA, which respectively state that the Act ‘shall apply to any serious offence or foreign serious offence’ and ‘shall apply to any property, whether it is situated in Singapore or elsewhere’, as well as from Section 2(1), which defines ‘criminal conduct’ and ‘drug dealing’ as the doing of such acts ‘whether in Singapore or elsewhere’.

ii 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 in relation to criminal investigations or proceedings to other states in respect of certain prescribed 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);
- requesting the attendance of a person;
- requesting the custody of a person in transit;
- the enforcement of a foreign confiscation order;
- search and seizure;
- locating or identifying persons; and
- service of process.

The Attorney-General’s Chambers handled 957 mutual legal assistance and extradition matters in 2017, compared with 1,126 in 2016.

**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 applies in respect of any of the 40 ‘declared Commonwealth countries’ or a ‘foreign State . . . between which and Singapore an extradition treaty is in force’.

Extradition is allowed only where the fugitive has committed an ‘extradition crime’ within the defined meaning of the EA. In the case of a declared Commonwealth country, this refers to an offence that is punishable with a maximum penalty of death or imprisonment for not less than 12 months and that is an offence described in the First Schedule to the EA. In the case of a foreign state, this refers to ‘an offence against the law of [. . . the] foreign State [where] the act or omission constituting the offence or the equivalent act or omission would, if [it had taken] place in or within the jurisdiction of Singapore, constitute an offence against the law in force in Singapore’ and that is an offence described in the First Schedule to the EA.

Embodied in the definition of an ‘extradition crime’ in the case of a foreign state 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’ (i.e., the court will look at the conduct alleged against the fugitive and determine whether the conduct would have been criminal had it been committed within the jurisdiction of the requested state). In this regard, the Singapore courts will not apply the ‘ingredients test’, which requires strict correspondence or identity of 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.

---

The MAS is signatory to a number of bilateral and multilateral memoranda of understanding (MOUs). Separately, the Singapore police force is a member of INTERPOL and has MOUs with, \textit{inter alia}, the police forces of Australia, Brunei, Hong Kong, and New York, and its Suspicious Transaction Reporting Office is part of the Egmont Group of Financial Intelligence Units. Various other Singapore agencies, such as the CPIB, the Casino Regulatory Authority 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 37-member intergovernmental standards-setting body that develops and issues guidelines on combating international money laundering and terrorist 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, 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 a bank or any information relating to any deposits of a customer of a bank.

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.

It should be noted that if a court order is obtained under the MACMA (see above), then the MACMA provides for civil and criminal immunity to any person who complies with the court order to produce any thing, and such production will not be treated as a breach of any restriction on disclosure (whether imposed by law, contract or rules of professional conduct).

V YEAR IN REVIEW

The past year has seen Singapore’s authorities increase their focus on the investigation and prosecution of corporate misconduct and, in particular, on criminal liability for companies.

In March 2018, Parliament passed the Criminal Justice Reform Bill. One of the key reforms is the introduction of deferred prosecution agreements (DPAs) into the criminal investigation and prosecution landscape in Singapore. Under the new statutory scheme, the

---

7 These include banking, securities and commodities regulators in Australia, Brunei, China, Malaysia, Myanmar, the United Arab Emirates, the United Kingdom and the United States.
8 These include the International Association of Insurance Supervisors and the International Organization of Securities Commissions.
9 This grouping consists of 152 financial intelligence units (FIUs), which include both national-level and local-level FIUs.
10 The most recent, the FATF Recommendations 2012, comprises some 40 recommendations. The FATF also periodically issues guidance and statements on specific issues and jurisdictions.
11 See Section 40A of the Banking Act.
12 See Section 13 of the Personal Data Protection Act 2012.
13 See Section 24(2) of the MACMA.
Public Prosecutor can enter into DPAs with companies, partnerships and unincorporated associations; individuals cannot enter into a DPA with the Public Prosecutor. Some notable features of the DPA regime include:

a. All DPAs will require approval by the High Court.
b. The High Court must be satisfied that entering into the DPA is in the interests of justice, and that the terms of the DPA are fair, reasonable and proportionate.
c. The terms of the DPA may include payment of a financial penalty, compensation to victims, a donation to charity, implementation or enhancement of compliance programmes, appointment of a court-designated person to supervise the subject’s internal controls, and cooperation in ongoing investigations.
d. As a general rule, a DPA is intended to be published and made public after it has been approved by the High Court.

The focus on criminal liability for companies was also seen in statements released by the CPIB earlier this year. The CPIB has reiterated its strong focus on private sector corruption, and emphasised that private sector cases continued to form the majority of all the cases registered for investigation by the CPIB in 2017.

The CPIB has made it clear that it will focus on private sector corruption cases in which company representatives give bribes to further the business interests of their respective companies. In March 2018, two companies were charged for being in a conspiracy with their own directors and shareholders in corruption-related offences, for allegedly making corrupt payments to the general manager of a town council as an inducement to advance the business interests of those companies. The CPIB has identified three areas that have continued to be of concern in recent years: construction, wholesale and retail businesses, and warehouse, transport and logistics services.

The MAS and the CAD announced an expansion of the scope of their joint investigation arrangement, and that it will henceforth jointly investigate all offences under the Securities and Futures Act and the Financial Advisers Act. The MAS and the CAD have been jointly investigating market misconduct offences since 2015. The increased scope of the joint investigation arrangement sends a strong signal that the Singapore authorities intend to enhance their investigative efforts in dealing with white-collar crime.

VI CONCLUSIONS AND OUTLOOK

Singapore has continued to safeguard its reputation as a corruption-free business environment, and it is expected to further emphasise its zero-tolerance stance towards corruption. The focus on corporate criminal liability suggests that investigation and enforcement activity will increasingly turn towards companies as the subject of investigations and prosecutions. This will be in line with the new DPA regime, which is only available to corporate entities. These factors are expected to significantly shape Singapore’s investigation and enforcement landscape in the coming year.
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 take 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 accused (identification and gathering of personal details), (2) determine the damage caused and (3) identify the person responsible.

Any investigative measures that violate fundamental rights (the interception of personal communications, searches of and dawn raids on private premises, etc.) 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 within the context of the investigation. The court must oversee the organisation and implementation of the measure.

Occasionally, 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, so that the necessary proceedings may be conducted or so that it may be ruled that there is no case to answer when it is found that there are insufficient grounds for bringing any action.

Additionally, given 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, and may also appear at preliminary investigation stages.

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

1 Mar de Pedraza is the managing partner and Paula Martínez-Barros is a senior associate at De Pedraza Abogados.
responsible for offences provided for by law, and impose penalties. These agencies are able to require the production of documents and to question 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.

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.

Finally, a company under investigation is not required to cooperate with authorities, but doing so is a mitigating circumstance of its criminal liability that can be applied under Article 31 quater b of the Spanish Criminal Code.

II CONDUCT

i Self-reporting

Act 5/2010 of 22 June 2010 entered into force in December 2010, amending Act 10/1995 of 23 November 1995 on the Criminal Code. One of the main developments of this new legislation was the inclusion for the first time of 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’, 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.

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; and terrorism offences (Title XXII, Chapter V).
Notwithstanding the foregoing, the latest reform introduced by 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:

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.

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 new 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.

---

3 Act 1/2015 of 30 March also adds to 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 to include the liability of legal persons (Penal Code, Articles 359 to 365); (5) Article 386 is amended so that Section 5 includes liability under Article 31 bis for crimes of counterfeiting; and (6) new Article 510 bis of the Penal Code introduces the liability of legal persons for crimes committed on the occasion of the exercise of fundamental rights and public freedoms guaranteed by the Constitution in relationship with provocation, hate or violence as defined in the new wording of Article 510 of the Penal 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 latest reform introduced by Act 1/2015 expressly sets the requirements for an effectual corporate compliance programme, including reporting channels facilitating the detection of possible risks and infringements to the authority entrusted with monitoring the operation and observance of the prevention model.

For these purposes, 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. Various different information sources may be used for warning of possible irregular conduct, for example, work carried out by the internal audit department, reporting channels, exit interviews, rumours and employee satisfaction surveys.

Once possible irregular conduct is known, the company will investigate it in accordance with the rules set out in its guidelines on internal investigations.

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.

When there is suspicion of the commission 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 counsel communications will be protected by professional secrecy in Spain. In-house counsels are bound to the company (the client) by means of an employment relationship and, therefore, are not considered independent. Thus, their communications with the entity might not be protected under legal privilege.

Professional secrecy should be maintained at all times in any documents (including communications) produced during an internal investigation, even though its scope under Spanish law is more limited than under English law. The professional secrecy of lawyers is enshrined in the right to personal privacy and the right to a fair defence, and releases them

---

4 Article 18.1 of the Spanish Constitution.
5 Article 24 of the Spanish Constitution.
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.

During 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.

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 the compliance officer regarding the specific case in question to ensure that the investigation is appropriate and proportionate, and respects the rights of all parties involved.

iii Whistle-blowers

From a criminal standpoint, the figure of the whistle-blower is fairly new in our system since the criminal liability of legal entities did not apply until 2010 and was not clearly regulated until the reform of 2015, when the impact that full implementation of compliance programmes will have on the liability of companies was specified in more detail.

For this reason, it is still too early to tell what position whistle-blowers will take regarding the reporting of illegal conduct to government authorities.

Note that there are no incentive programmes for whistle-blowers for reporting wrongdoings to the authorities. Nevertheless, if the whistle-blower is a wrongdoer and becomes an accused party to the criminal proceedings, his or her penalty might be mitigated by the court for reporting the illegal acts to the authorities, according to Article 21.5 of the Criminal Code (confess the illegal act to authorities).

Lastly, there are no specific protections in place for whistle-blowers, any more than it is guaranteed that their reports will be confidential. It is still not fully clear whether whistle-blowers can preserve anonymity or not.

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 (1) no specific individual perpetrator of the offence has been found, or (2) 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

6 Article 263 of the Criminal Procedure Act.
7 Articles 416.2 and 707 of the Criminal Procedure Act.
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, since 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 individuals and vicariously.

**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 3 ter 1, 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, note that the range of potential sanctions will not vary based on the authority bringing the action.

---

8 Article 116.3 of the Criminal Code.
9 Article 120 of the Criminal Code.
iii Compliance programmes

It has already been noted that Act 1/2015 of 30 March amending the Penal Code entered into force in July 2015.

This amendment expressly acknowledges that a legal person may be exempted from criminal liability if it has a corporate compliance programme for the prevention of crime. This acknowledgement puts an end to all discussion on the matter, and for the first time establishes 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 representatives of a legal person, the new Article 31 bis 2 of the Penal Code makes the following conditions necessary in order for the enterprise to be exempted from criminal liability:

a 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 employees (or other persons under the authority of the de facto or de jure directors and legal representatives), 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

---

10 As seen above, the new Article 31 bis 1a changes the previous wording 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’.
11 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.
12 The application of this Article in practice will enable us to ascertain the exact scope of this concept.
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;

d 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;

e 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

f 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.

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) since 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 in order 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.
As regards measures that may be taken against employees, an effective corporate compliance programme must include a disciplinary system that suitably penalises the breach of measures established in the model. As described above, a disciplinary system is expressly provided for in Act 1/2015.

IV INTERNATIONAL

i Extraterritorial jurisdiction

Act 5/2010 and Act 1/2015 do not explicitly set out provisions regarding the extraterritorial jurisdiction of the Spanish courts in the event of the application of Article 31 bis of the Criminal Code. Thus, any reference to perpetrators of an offence – Spanish and foreign – contained in the rules on extraterritorial jurisdiction set out in Article 23 of the Spanish Act on the Judiciary must be extended to legal entities.

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, Spanish Act 1/2014 of 13 March on universal justice amended Spanish Act 6/1985 of 1 July on the judiciary, specifically the wording of Article 23.4. This amendment introduced the possibility of the Spanish courts hearing and prosecuting offences of corruption between individuals13 and offences of corruption in international business transactions,14 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;

13 Article 286 bis of the Criminal Code.
14 Article 286 ter of the Criminal Code.
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.

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:

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, note that Spain only grants extradition in compliance with a treaty or the law, in accordance with the principle of reciprocity. In addition, the requirement of dual criminality must be met, in other words, 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 the European Convention on Extradition and to a large number of bilateral treaties on extradition.

iii Local law considerations

Provisions exist that may restrict investigations involving multiple jurisdictions. The most relevant law in this regard is probably the Personal Data Protection Act.

In certain cases, however, this Act warrants and authorises the processing or transfer to third parties of personal data without the consent of the owner. In this regard, Article 11, relating to the disclosure of data to third parties, provides that the consent of the owner of the data is not necessary, inter alia, ‘when the disclosure that must be made is to the Ombudsman, the Public Prosecutor’s Office or judges or courts or the Court of Auditors, in exercise of the functions conferred thereon’.

As regards banking secrecy, this is not regarded under law as an asset or property that merits 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, notwithstanding that 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 as a consequence of internal wrongdoings.

To date there have been 12 judgments by the Supreme Court regarding the criminal liability of legal persons. None of the companies had a compliance programme implemented, or compliance officers, code of ethics and the like.

On 29 February 2016, the pioneering Supreme Court sentence confirming the criminal liability of a corporation was delivered (STS 154/2016). The ruling provided guidelines for legal entities to comply with the law and norms through the implementation of models of prevention and control according to Article 31 bis of the Criminal Code so as to avoid penalties.

Two judgments from the Supreme Court about the criminal liability of legal persons – on 16 March 2016 (STS 221/2016) for property embezzlement and on 13 June 2016 (STS 516/2016) for crimes against environment – ruled that the legal person could not be criminally responsible because the illegal acts took place before the reform of the Criminal Code.

Rulings STS 154/2016 and 221/2016 of the Supreme Court warned about the future conflicts of interest that may arise between the accused natural person (that represents the legal person) and legal persons who are represented in court by the same counsel, which may cause a breach of the right to defence of the legal entity.

Without prejudice to the court affirming that there is no general answer for this question, 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.

Another matter analysed in these 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.

The following rulings by the Supreme Court did not shed light on interpreting the criminal liability of legal persons: STS 740/2016 of 6 October; STS 4728/2016 of 3 November; STS 31/2017 of 26 January, in which the company could not be held responsible and was just declared vicariously civil liable; and STS 121/2017 of 23 February, which acquitted the company of a crime against workers’ rights as the conviction of a legal person for such an offence is not possible according to the Penal Code.

One remarkable ruling of the Supreme Court was STS 583/2017 of 19 July, which upheld the criminal liability of six companies for money laundering offences (and against public health), but lowering the penalties imposed by the lower court (Audiencia Nacional).
This sentence confirmed previous Supreme Court case law and definitively established 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.

VI CONCLUSIONS AND OUTLOOK

As has already been discussed, the criminal liability of legal entities is quite new in Spanish legislation and there is little case law in this regard.

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 likely we will have more rulings from superior courts in such matters.

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;
- attorney–client privileges that may apply during internal investigations;
- the impact of the collaboration with authorities;
- the personal liability of compliance officers for not fulfilling their duties;
- conflicts of interest between legal and natural persons; and
- the application, in practice, of mitigating and exonerating circumstances and the like.
Chapter 22

SWEDEN

Ulf Djurberg and Sofie Ottosson

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 crimes and closely related offences. The Unit consists of 10 specialist prosecutors and three economic accountants. 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 strengthening the anti-bribery and money laundering legislation. On 1 June 2012, important changes were made in the Penal Code to provide clearer and more appropriate bribery legislation. An act ensuring the protection of whistle-blowers was adopted in January 2017. Furthermore, the focus in the European Union to provide tools to fight organised crime has resulted in the implementation of a fourth anti-money laundering directive, which applies to a larger number of operators than the previous directives and includes a few additional obligations for entities covered by the directive.

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 crimes such as insider trading. High-profile cases in the past two years include dawn raids at the premises of several insurance companies and companies in the construction sector. Further, the Swedish Tax Agency has many different tools to ensure compliance with tax rules, such as, *inter alia*, unannounced control visits.

The Environmental Code regulates criminal conduct against the environment, offences that are primarily committed in the course of company activities. Included in the listed ‘penalty provisions’ are different kinds of pollution, causing environmental disturbance.

---

1 Ulf Djurberg is a partner and Sofie Ottosson is an associate at Setterwalls Advokatbyrå AB.
environmentally hazardous handling of chemicals, unauthorised environmental activity and obstruction of environmental control. The Environmental Code is supervised by several authorities, including the Swedish Environmental Protection Agency, the Surgeon General of the Swedish Armed Forces, county administrative boards, municipalities and other government agencies.

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.

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 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 made 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. However, as shown by the TeliaSonera case (see Section V.ii), it is often in the best interests of a company that has been accused of illegal conduct for it to disclose its findings to the general public in order to restore public trust.

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 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.
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.

The Swedish Corporate Governance Board promotes good corporate governance within listed companies. A major part of the Board’s role is management of the Swedish Corporate Governance Code, which was introduced on 1 July 2005 and last amended on 1 December 2016. 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**

Both natural and legal persons may be held liable for breaches of Swedish 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 in order to be granted. Needless to say, responsibility may also be claimed on the basis of contractual obligations.
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.

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. The representative may also be held criminally liable for conduct within the company’s scope of business. 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.

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 kronor and 10 million kronor for crimes committed in the exercise of its business operations, if the corporation has not properly prevented the crime, or where the crime has been committed by persons supervising or controlling the business. It has recently been proposed to increase the maximum corporate fine from 10 million kronor to 100 million kronor for larger companies (with more than 50 employees and a minimum turnover of 80 million kronor).

It should be noted that 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, a corporate fine was imposed in about 15 per cent of cases in 2017 and the highest fine was 150,000 kronor.

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.

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. According to the Corporate Governance Code, which applies to all Swedish companies whose shares are listed on a regulated market in Sweden, 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. Jurisdiction also exists where the crime was directed towards a Swedish legal or natural person. Note that, 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 Sweden, 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 the crossing of an external border. 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

The Swedish legislative framework on corruption prevention was reviewed by the Council of Europe in 2013. In the subsequent report, the GRECO anti-corruption unit of the Council of Europe stated that Swedish legislation on the prevention of corruption works quite well in general. This was assumed to be a result of the Swedish principle of public access and the fact that Sweden has several state and private institutions that aim to control whether public authorities and market actors comply with laws and regulations. Nevertheless, the Council of Europe still considered that Swedish legislation on the prevention of corruption needed to be strengthened. It recommended Sweden should take measures regarding a number of areas and to introduce them during Spring 2015 at the latest.

Some of the changes recommended by the Council included new legislation that further ensures independence, impartiality and integrity of lay judges. The recommendations involved a system for proper guidance on ethical questions and training for the lay judges in matters regarding ethics and corruption. It was also suggested that a code of conduct directed at the members of Parliament be introduce to encourage a more proactive attitude concerning ethical questions and the identification of conflict of interests. For example, mandatory disclosure of potential conflicts of interest was recommended as well as clearer rules on gifts to members of Parliament.

The Council concluded in its second compliance report, adopted in October 2017, that Sweden has implemented satisfactorily or dealt with in a satisfactory manner six of eight recommendations in the evaluation report and that the two remaining recommendations have been partly implemented. Subsequent to the report, several measures have been taken to better ensure the independence, impartiality and integrity of lay judges, including legal amendments making it easier to dismiss lay judges who are not suited for the assignment, as well as obligatory training on topics such as ethical conduct and conflicts of interest. The government has also adopted a code of conduct for members of Parliament as suggested by the Council. The code contains a part dedicated to gifts and the requirement that members of Parliament must report gifts received in their official capacity to the Internal Service Department. A new act regulating the registration and processing of gifts received by members of Parliament has also been adopted, imposing an obligation on all members of Parliament to register gifts received in connection with their role.

However, mandatory disclosure of potential conflicts of interest has not been introduced and the Council thus finds that its recommendation in this regard is only partly implemented. Furthermore, the Council finds it regrettable that supervision of the code of conduct has not been entrusted to a mechanism capable of imposing sanctions to ensure its enforcement.

ii Cases

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 involve corruption crimes in connection with telecommunications company TeliaSonera’s establishment of business in Uzbekistan. The affair has not only forced several members of the management team (including the CEO) and the board of directors to resign because of the mere suspicion of acts of bribery by TeliaSonera officials in relation to the company’s business activities in Uzbekistan, but also the former CEO was denied discharge from
liability at the annual general meeting in April 2014. The fact that the shareholders denied the CEO discharge from liability is a very unusual measure with respect to a Swedish ‘large cap’ listed company.

Another prominent case is Bombardier, which involves alleged corruption crimes in connection with a procurement of railway services in Azerbaijan in 2013. Bombardier participated in the procurement with another company within the Bombardier group and a third Azerbaijani company, combined as a consortium. A representative of the Azerbaijani company was employed by the contracting authority at the time for the procurement and had close contact with a Bombardier business development manager during the procurement. The business development manager was alleged to have included the Azerbaijani company in the consortium in order for the consortium to gain advantages in the procurement process and to be awarded the contract. The Bombardier business development manager was prosecuted in August 2017 for gross bribery, but was acquitted by the Stockholm district court in October 2017 since the prosecutor could not provide enough evidence to prove that the Azerbaijani company had been included in the consortium for the exchange of advantages in the procurement process. The case has been appealed to the Svea Court of Appeal.

VI CONCLUSIONS AND OUTLOOK

Sweden is traditionally considered to be one of the least corrupt countries in Europe. In 2017, it was ranked the sixth least corrupt country in the world, according to Transparency International’s Corruption Perceptions Index, a result that indicates a comparatively low level of corruption but which may still be considered alarming in light of the fact that Sweden has not been ranked higher than the fifth least corrupt country in the world since 2006. It is possible that the result has been affected by the substantive number of media reports during 2017 and 2018 regarding suspected corruption among several Swedish public authorities. However, whether corruption in Sweden has actually increased is a question that is yet to be answered.
Chapter 23

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:

a. offences committed against persons protected by international law;

b. offences committed against federal magistrates;

c. acts infringing Switzerland’s sovereignty, neutrality or economic interests;

d. offences that pose a severe threat to the public; or

e. 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.

---

1 Bernhard Lötscher is a partner and Aline Wey Speirs is a counsel at CMS von Erlach Poncet Ltd.
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).
The authority generally competent at the federal level to investigate and prosecute criminal conduct is the Office of the Attorney General. Matters in the field of 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.

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.
FINMA has no powers to impose penal sanctions such as fines. However, it may respond to contraventions of regulatory rules with severe administrative measures.\(^\text{17}\)

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. Since 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.

---

\(^{17}\) See: Articles 31 \textit{et seq}. FINMASA.

\(^{18}\) Federal Act on Cartels and Other Restraints of Competition (SR 251).

\(^{19}\) See, in particular, Articles 40 and 42 of the Cartel Act (CartA).

\(^{20}\) 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.

\(^{21}\) Article 113, Paragraph 1 CPC.

\(^{22}\) 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).

\(^{23}\) 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.

\(^{24}\) Pursuant to Article 102, Paragraph 2 CC, undertakings may be held criminally liable for participation in a criminal organisation (Article 260 \textit{ter} CC), financing of terrorism (Article 260 \textit{quinquies} CC), money laundering (Article 305 \textit{bis} CC) and bribery (Articles 322 \textit{ter}, 322 \textit{quinquies}, 322 \textit{septies}, Paragraph 1 or 322 \textit{octies} CC).

\(^{25}\) Articles 74 \textit{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.

For undertakings active in the field of financial intermediation 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. 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. 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. 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.

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

---

26 Financial intermediaries include banks, investment companies, insurance companies, securities traders, central counterparties and securities depositories, providers of payment services, casinos and asset managers.
27 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.
28 Article 29, Paragraph 2 FINMASA.
29 Article 49a, Paragraph 2 CartA.
30 See: Ordinance on Sanctions Imposed for Unlawful Restraints of Competition (Cartel Act Sanctions Ordinance, SR 251.5).
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 in order 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, 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 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.

---

32 See: Article 717 CO.
33 Articles 328 and 328b CO.
34 Federal Act on Data Protection (FADP, SR 235.1)
35 Articles 12 et seq. FADP.
36 Article 321a, Paragraph 1 CO.
37 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.
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 ‘outsource’ investigations and the keeping of records of an investigation’s results to law firms in order 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

In the private sector there is no specific law on whistle-blowing. An attempt by Parliament to introduce provisions to existing legislation failed in 2015. Hence, the general rules and principles of employment law, company law, criminal law and data protection law apply.

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; otherwise the employee may be in breach of contractual loyalty and confidentiality obligations towards the employer. If the disclosure is made intentionally, criminal liability may ensue in addition to the liability for breach of contract.

Swiss law does not require undertakings to set up a specific internal whistle-blowing unit to which employees may report confidentially, although, 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 11 per cent of all companies in Switzerland have introduced a reporting point. Considerable differences exist between large international corporations where the majority of the designated internal or external reporting points are to be found (70 per cent) and smaller to medium-sized enterprises where such reporting points are still rare (less than 10 per cent).

The case law of the Federal Supreme Court provides additional 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.

---

40 See: DFT 127 III 310, 30 March 2011, consid. 5.
41 Article 22a Federal Act on Personnel (BPG, SR 172.220.1).
42 See: www.efk.admin.ch/de/whistleblowing-d.html.
In 2017, the federal government introduced an official and secured digital platform where public employees or private persons may report suspected misconduct anonymously.\(^{43}\) Since the introduction of the platform, the number of reports has increased significantly.\(^{44}\)

The Swiss Federal Police (Fedpol) is operating a web-based platform for reporting suspected corruption.\(^{45}\) The platform safeguards the anonymity of the person reporting and neither stores the IP addresses, time or 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.\(^{46}\)

Non-governmental 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.\(^{47}\)

While the enactment of whistle-blower legislation in Switzerland is stalled, guidelines and recommendations for compliance and best practices shape the reality. Swiss companies are well advised to establish reporting systems, endorse company policies for transparency and to draft rule books and guidelines for their employees.

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.\(^{48}\) 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.\(^{49}\)

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

---

\(^{43}\) See: www.whistleblowing.admin.ch.

\(^{44}\) From around 70 reports in previous years to 122 reports in 2017.

\(^{45}\) See: https://fedpol.integrityplatform.org.


\(^{48}\) Article 102, Paragraph 1 CC.

\(^{49}\) Article 102, Paragraph 2 CC.
the undertaking itself and may therefore expose the undertaking to civil liability. 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. 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.

ii Penalties

Undertakings may be fined up to 5 million Swiss francs for criminal conduct that occurs in their domain. 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.

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. In 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.

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. 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 which the undertakings concerned have achieved.

---

50 Article 55, Paragraph 2 Civil Code.
51 Article 55, Paragraph 1 CO.
52 Article 754 CO.
53 Article 102 CC.
54 Articles 70 et seq. CC.
55 Articles 31 et seq. FINMASA.
56 Articles 44 et seq. FINMASA.
57 Articles 49 and 50 CartA.
in Switzerland. 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. In addition, COMCO may fine individuals up to 100,000 Swiss francs.

### 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.

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.

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.

### iv Prosecution of individuals

As noted above, criminal law primarily addresses the conduct of individual perpetrators. Liability of undertakings is basically 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. Consequently, action against individuals is an increasingly common feature of regulatory proceedings.

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

---

58 Article 51 CartA.
59 Article 52 CartA.
60 Articles 54 et seq. CartA.
61 Article 102, Paragraph 2 CC.
64 FINMA guidelines on enforcement policy of 25 September 2014.
investigation, non-disclosure of relevant evidence, incomplete or misleading fact statements or the like may amount to unlawful assistance to evade prosecution. Furthermore, prosecuting authorities may, and often do, impose a duty of confidentiality on witnesses.

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, 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. 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.

IV INTERNATIONAL

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 Organisation for Economic Co-operation and Development (OECD), and aims to safeguard against the infringement of human rights by corporations.

In the public law domain, it is the Act against Unfair Competition, the CartA, the Data Protection Act and the Public Procurement Act 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). Similarly, competition law offences that have an effect in Switzerland can be investigated and sanctioned by COMCO even if they took place abroad.

66 Article 305 CC.
67 Article 165 CPC.
68 Articles 321a and 321d CO.
69 See: Article 328, Paragraph 1 CO.
71 Federal Act Against Unfair Competition (UCA, SR 241).
72 Federal Act on Public Procurement (SR 172.056.1).
73 Articles 3 and 7 UCA.
Criminal law follows the principle of territoriality, but extends its reach with respect to certain offences. In 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.

Parliament is scheduled to debate 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. Should the proposed regulation become law, governance breaches by Swiss undertakings abroad would generally 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. The distinction of these two routes of cooperation is important. In a recent judgment, 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 required for the purposes of criminal prosecution must be sought by way of judicial assistance in criminal matters. 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). There is no extradition of Swiss nationals against their will, but foreigners can be extradited under respective international treaties or the IMAC.

FINMA cooperates with foreign supervisory authorities in specific supervisory or enforcement proceedings. The latest statistics (published in 2015) show a steady increase in the number of requests for international cooperation 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 anti-competitive cross-border activities.

---

74 The initiative is known as ‘Konzernverantwortungsinitiative’; see: http://konzern-initiative.ch.
75 The Swiss government maintains a comprehensive database on the sources of law and forms relevant in international legal assistance, https://www.rhf.admin.ch/rhf/de/home/rechtshilfefuehrer/laenderindex.html.
76 Federal Supreme Court judgment dated 28 December 2017, 2C_640/2016.
77 Federal Act on International Mutual Assistance in Criminal Matters (SR 351.1).
78 Article 32 of the International Mutual Legal Assistance Act.
79 See: https://www.finma.ch/de/durchsetzung/amthilfe/internationale-amthilfe/.
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. The criminal sanction may also apply to foreign attorneys travelling to Switzerland for the purpose of an investigation\(^\text{81}\) and it 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.\(^\text{82}\) It applies also to the intra-group and cross-border disclosure of 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.

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\(^\text{83}\) and any breach is sanctioned by criminal law.\(^\text{84}\) However, the concept of legal privilege is fairly narrow and does not encompass legal advice from in-house counsel or external legal experts who are not members of the Swiss Bar.\(^\text{85}\)

V YEAR IN REVIEW

The world of soccer kept the Office of the Attorney General (OAG) busy throughout 2017. On 20 March 2017, the federal prosecuting authority opened a new file against a former secretary general of FIFA and others for alleged bribery, fraud and criminal mismanagement in connection with the assignment of broadcasting rights for the 2018, 2022, 2026 and 2030 World Cup tournaments. In June 2017, the OAG completed a first proceeding in the context of the FIFA investigations by way of a summary penalty order. The accused, a former employee of a Swiss bank, was found guilty of forgery of documents pursuant to Article 251 CC and contravention of diligence duties under the AMLA. The case is remarkable as it was handled in close coordination with the United State Attorney's Office for the Eastern District of New

\(^{81}\) Spehl/Gruetzner (eds.), Corporate Internal Investigations, C H Beck oHG, Munich 2013, Germany, p. 360 n 25.

\(^{82}\) Ibid., p. 361 n 29.

\(^{83}\) Article 13 Federal Act on Free Movement of Attorneys (BGFA, SR 935.61).

\(^{84}\) 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.

\(^{85}\) 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.
York, in terms of both timing and sanctioning. The counts to which the accused had pleaded guilty in the US proceedings were no longer prosecuted in Switzerland in order to avoid double-jeopardy issues.

In March 2017, the OAG closed a noteworthy case of self-reporting in a corruption matter. In 2015, the accused undertaking reported suspected bribe payments to Nigerian officials. When assessing the case, the OAG gave particular consideration to elements such as self-reporting, active cooperation from the outset, comprehensive support of the investigation and implementing concrete measures to remedy organisational deficits. The company was eventually sentenced to a symbolic fine of 1 Swiss franc and disgorgement of unlawful profits in the amount of 35 million Swiss francs.

In the area of financial market law enforcement, FINMA has continued its efforts to deter money laundering by focusing on compliance with diligence duties. In line with the enforcement strategy as published in October 2014, individuals responsible for breaches stayed in the focus of regulatory action – indeed, the number of sanctions imposed on individuals roughly doubled the number of orders made against undertakings in the segment of unauthorised banking and security trading activities.

As in 2016, suspected and actual involvement of Swiss financial institutions in global corruption and money laundering scandals surrounding 1MDB, FIFA and Petrobras were another focal point of FINMA investigations. A notable case completed in January 2017 concerned a bank that accepted transfers between 2006 and 2015 from the entourage of 1MDB totalling US$2.4 billion, thereby ignoring a series of indicia of money laundering. Besides a declaratory ruling blaming the bank for the misconduct, FINMA confiscated illicit profits in the amount of 6.5 million Swiss francs.

Other significant areas of regulatory action were the fight against insider trading and market manipulation, and the prevention of unauthorised business activities that are reserved for licensed banks and security traders.

Last but not least, in September 2017, FINMA ordered for the first time the liquidation of a cryptocurrency undertaking. The coin offering was found to qualify as a disguised taking of deposits from the public, which required a banking licence. Moreover, the currency was not immune to price manipulation.

While the focus of investigations by COMCO in 2017 remained on hard cartels, such as agreements to fix prices, agreements to limit the quantities of goods or services to be produced, purchased or supplied or agreements to allocate markets, the most significant case concerned the abuse of a dominant position in the market. Swiss Post, the state-owned provider of postal services, was charged in December 2017 a penalty of 22.6 million Swiss francs for having discriminated against clients by applying different price models and for having obstructed competitors.

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. To name a few:

a Attorney–client privilege in connection with internal investigations: case law appears to be in flux as regards the prerequisites for, and scope of, protection of attorney work products in internal investigations.
Protection of whistle-blowers: as already discussed in Section II.iii, a legislative project by the government was rejected in Parliament in 2015. Swiss law thus still fails to provide specific guidance for undertakings and individuals concerned.

Multi-jurisdiction 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-jurisdiction 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.
I INTRODUCTION

The Royal Thai Police (the police) is the main investigating authority empowered by the Criminal Procedure Code to conduct an investigation on criminal cases. However, in certain cases, the Department of Special Investigation (DSI), often referred to as the Thai FBI, is empowered to conduct investigations on ‘special cases’ as prescribed by the Special Case Investigation Act BE 2547 (2004), which include certain cases under the Revenue Code, customs law, excise law, the Foreign Business Act, the Computer Crime Act, the Board of Investment Commission Act, the Copyright Act, the Patent Act and the Trade Competition Act.

The police and the DSI have similar investigatory powers, although the DSI has additional powers in certain areas. In exercising their powers, both entities are subject to the Criminal Procedure Code and the protections provided to alleged offenders under its provisions.

Specific legislation may also empower government authorities to investigate matters under their supervision. For example, the new Customs Act BE 2560 (2017) (the Customs Act) empowers the Customs Department to conduct searches and seizures;2 the new Trade Competition Act BE 2560 (2017)3 empowers the Office of the Trade Competition Commission (OTCC) to summon any person to give statements, facts, or make a clarification in writing, and to conduct searches and seizures for examination purposes; the Foreign Business Act BE 2542 (1999) (FBA) empowers officials of the Ministry of Commerce to investigate by issuing an enquiry letter or summoning a person to give oral testimony;4 and the Organic Act on Counter Corruption BE 2542 (1999) empowers the National Anti-Corruption Commission (NACC) to investigate allegations that a political office holder or a government official is unusually wealthy, corrupt or guilty of malfeasance in office.

In practice, businesses generally cooperate with government authority investigations to avoid more excessive measures or future inspections. It is also the case that Thai laws generally provide penalties for failure to cooperate with government requests or to facilitate the conduct of investigations. Nonetheless, if a business considers that the measures taken

---

1 Melisa Uremovic and Visitsak Arunsuratpakdee are partners at R&T Asia (Thailand) Limited.
4 Section 30 of the FBA: The Registrar and competent officials have the following powers: (1) to address in writing enquiries or summons requiring any person to give explanations on any facts and furnish documents or evidence necessary for factual examination . . .
by the government authority are unreasonable or unlawful, it may take an adversarial stance against the authority. In addition, businesses may reserve the right to challenge the inspectors’ authority to take certain documents on the grounds of either relevance under the terms of the warrant or authority or, to a lesser extent, legal privilege (for documents held by lawyers).

Even though it is unclear to what extent political agendas or domestic priorities have an impact on investigations, governmental authorities often perform in accordance with the policies of the government. For example, in February 2015, the European Union put Thailand on formal notice for not taking sufficient measures to tackle illegal, unreported and unregulated (IUU) fishing, making the elimination of IUU fishing a priority issue. Therefore, the government has requested that the relevant authorities (the Marine Police Division, the Royal Thai Navy and the Customs Department) give it their full cooperation in supporting implementation of the IUU fishing elimination plan formulated by the Ministry of Agriculture and Cooperatives, and, in March 2018, the government appointed special arrest teams to inspect fishing-related crimes at sea. This is a case in point of how political agendas or domestic priorities affect governmental authorities and any resulting investigations in Thailand.

II CONDUCT

i Self-reporting

Thai laws generally do not include a self-reporting requirement in the event of wrongdoing. It is also generally the case that self-reporting does not reduce applicable penalties. Individual regulators may introduce their own self-reporting mechanism, for example, the Customs Department’s voluntary audit programme (VAP). The VAP is a self-reporting or self-review programme initiated to foster good relationships between the Customs Department and the business sector, by allowing businesses to pay deficit duty and the Customs Department to consider waiving penalties and surcharges. While the VAP is not supported by a specific legislative provision, case law supports the potential waiver of penalties in the event that the plaintiff has provided documentation and evidence to the post-audit officer that indicates no intent to evade tax. The key limiting factor for use of the VAP is that it is not valid if the Customs Department believes there was an intent to evade tax.

The existence of settlement programmes may encourage self-reporting, particularly as a settlement would typically indemnify the offender against any further prosecution on account of the offence and may also provide a significant reduction in penalties. For example, Section 256 of the new Customs Act provides a mechanism for the settlement of alleged offences upon payment by the alleged offender of the amount as negotiated and agreed between the alleged offender and the Customs Department. The settlement amount represents a substantial reduction of the total fines payable in the event of a successful prosecution of the offence. Leniency programmes are currently not well developed under Thai law.

---


© 2018 Law Business Research Ltd
Thai businesses may conduct internal investigations as they deem appropriate and there is no requirement to share the results of an internal investigation with any government body.

The Labour Protection Act BE 2541 (1998) provides that, during the investigation of an offence allegedly committed by the accused employee, the employer is not permitted to suspend an employee from work unless there are work rules or an employment agreement specifying that the employer has the right to do so. If there is such language in the work rules or employment agreement, the employer shall issue a written order of suspension to the accused employee stating the offence allegedly committed and a suspension period not exceeding seven days. The employer shall pay the employee not less than 50 per cent of the working day wages received by the employee prior to the suspension. If it appears that the employee is not guilty, the employer shall pay wages to the employee equivalent to the wages of a working day starting from the date of suspension. There is no law requiring that the employer provides the employee with legal representation during the investigation.

Investigations are typically conducted by internal counsel with support from external counsel in certain situations, for example, when the case involves violations of law or regulations. If a lawyer has been retained for the purpose of the internal investigation, the confidential information that the lawyer received from or provided to the client in the internal investigation shall not be disclosed. The disclosure by a lawyer of any confidential information about a client may be a violation of Section 323 of the Criminal Code.\(^7\)

Thailand does not have a specific law on whistle-blower protection, although it has been implemented under certain legislation (i.e., the Securities and Exchange Act and the Organic Act on Counter Corruption). Section 89/2 of the Securities and Exchange Act\(^8\) provides that employees who give information, cooperate or give assistance by any means to the competent authorities under the Act shall not be subjected to unfair treatment by the employer. Similar language appears in Section 103/2 of the Organic Act on Counter Corruption, which provides a protective measure to assist a person who discloses information regarding the dishonest performance of duties, unusual wealth, or other information that is beneficial for the performance of the NACC.\(^9\) In practical terms, whistle-blower reports of potential illegal conduct are rarely submitted to government authorities.

---

\(^7\) Section 323 of the Criminal Code: Whoever knows or acquires a private secret of another person by reason of his functions as a competent official or his profession as . . . a lawyer . . . and then discloses such private secret in a manner likely to cause injury to any person, shall be punished with imprisonment not exceeding six months or fined not exceeding ten thousand Baht, or both. Available at https://www.unodc.org/res/cld/document/tha/criminal-code-as-of-2008_html/Thailand_Criminal_Code.pdf.


\(^9\) Section 103/2 of the Organic Act on Counter Corruption: In the case where the NACC deems that any case warrants a protective measure to assist a person making the accusation, an injured person, a person making a request, a person giving a statement or a person who informs a clue or any information relating to the dishonest performance of duties, unusual wealth or other information which may be beneficial for actions to be taken pursuant to this Organic Act, the NACC shall inform the relevant agencies to take action for a protective measure against such person. Such person shall be deemed as a witness being entitled to the right for protection under the law on protection of witnesses in criminal cases. The NACC shall also submit a view as to whether the situation warrants a general measure or a special measure under such law for those persons . . .
Legal protection for witnesses is prescribed by the Witness Protection Act, in which the witnesses and relatives in criminal proceeding shall receive special protection measures in respect of cases related to offences under the laws on narcotics, money laundering, anti-corruption, customs, etc. In addition to corruption cases, Section 103/6 of the Organic Act on Counter Corruption provides immunity from prosecution to the person who provides information that can be used to determine there has been a commission of an offence by a State official.

In relation to the incentives programme for whistle-blowers, only specific legislation may empower government authorities to grant rewards for public participation in crime prevention. For example, Section 255 of the new Customs Act empowers the director general of the Customs Department to order the payment of money as bribe and reward to customs officials and third-party whistle-blowers for reporting under any offences thereof. Section 103/3 of the Organic Act on Counter Corruption empowers the NACC to grant a reward to informants who report information concerning corruption, unusual wealth or other beneficial information to NACC officials. Another example is that the Office of the Narcotics Control Board is empowered to grant rewards to informants who give information in drug cases.

III ENFORCEMENT

i Corporate liability

As the concept of piercing the corporate veil is not explicitly provided for by law, shareholders of a limited company or partners in a limited partnership have liability up to the amount of the unpaid value of shares or capital invested in the company or the partnership, as the case may be. Under Thai law, a juristic person (i.e., an entity recognised by law, such as a company or partnership) may be subject to both civil and criminal liability.

With regard to civil liability under the tort regime, to consider whether a juristic person is liable for the conduct of its employees, the Civil and Commercial Code (CCC) provides that an employer is vicariously responsible for its employee if the employee's action

---

10 Section 6 of the Witness Protection Act: In a case where a witness loses his/her security, a competent official from criminal investigation, interrogation, prosecution or the Witness Protection Bureau as the case may be shall design for the witness protection measures as deemed appropriate or as requested by the witness or other concerned party. Where necessary the said person may request a police officer or other official for protection and this must be subject to the witness's consent . . .

11 Section 103/6 of the Organic Act on Counter Corruption: Any person or accused who took part in the commission of offence with a State official as other accused, if he or she gives a statement, or informs a clue or provides information which is substantive and can be used as witnesses and evidence in the determination of fault in the commission of offence of such other State official, the NACC may deem it appropriate to keep that person as a witness without being prosecuted, pursuant to the criteria, procedures and conditions as prescribed by the NACC.


13 Section 103/3 of the Organic Act on Counter Corruption: The NACC shall provide for a reward to a person under Section 30 or may provide for any other remuneration or benefit to a person under Section 103/2, Paragraph 1, as the case maybe . . .

14 The Prime Ministerial Office Regulation Re: Rewards in Narcotics Case BE 2537 (1994).
is attributable to his or her employment. Vicarious liability can be established only for the relationship between an employer and an employee under an employment agreement with remuneration. Therefore, if such a link could be established, a juristic person employer will almost always be responsible for the actions of its employee, unless it can prove that the action is not attributable to the course of employment. The court usually interprets ‘course of work’ in an expansive manner to include, for instance, conduct that does not relate to work but occurs during working hours, or does not follow directions given by the employers but the ultimate objective of the action is for the benefit of the employers. This interpretation places a high burden on a company. Another key point to consider is that, even though the employee's conduct is not attributable to the 'course of work’ of an employer, a company may still be held liable under the principle of ‘agency by estoppel' enshrined in the CCC. For example, the company may be held responsible for the conduct of the employee that is not considered as the 'course of work' of an employer if the company explicitly or implicitly accepted such conduct.

At present, there are no general legislative provisions that define the principles governing the criminal liability of a juristic person. As a juristic person is represented and managed by a director or directors who are elected by the shareholders, where a company has conducted an unlawful act, it can only be subjected to a particular penalty (e.g., a criminal fine) owing to its nature. Certain laws explicitly impose criminal liability on a juristic person if it breaches its duties. For example, the Securities and Exchange Act BE 2535 (1992) imposes a fine on any company that violates the regulations issued by the Securities and Exchange Commission.

In an exceptional circumstance, the Supreme Court has ruled that a company is criminally responsible for manslaughter. In this case, the court held that the juristic person and its representative acted in gross negligence for failure to comply with the ministerial regulations. Although its employee was the person driving a gas tanker that was involved in an accident and caused a gas leakage and explosion resulting in high casualties, the court decided that the action arose through gross negligence. The Court also applied a standard of care higher than a reasonable man test. This case resembles corporate manslaughter liability under English law.

There is no specific legislation prohibiting a company and an individual from being represented by the same counsel. In practice, if there is a risk that the interest of the individual and the interests of the company may conflict, it is advisable that separate counsel be appointed.

---

15 Section 425 of the CCC: An employer is jointly liable with his employee for the consequences of a wrongful act committed by such an employee in the course of his employment.

16 Section 821 of the CCC: A person who holds out another person as his agent or knowingly allows another person to hold himself out as his agent, is liable to third persons in good faith in the same way as such person was his agent.


18 Judgment of the Supreme Court No. 3446/2537.
ii Penalties

The range of sanctions available against businesses in Thailand include fines (both administrative and criminal), confiscation of property and revocation of licences, based on the offence committed. ¹⁹

Recent legal amendments have clarified that, when an offender is a juristic person, if the offence of the juristic person derives from an order or an action of a director or a manager or any person who is responsible for the operations of the said juristic person, or where the said person has the duty to issue an order or to take an action but failed to do so and thereby caused the said juristic person to have committed the offence, the said person shall also be liable for the punishment provided for the offence. ²⁰

Apart from criminal penalties, a juristic person may be subject to administrative fines if he or she violates or does not comply with an administrative order imposed by an administrative agency. The general regulation governing administrative fines is the Administrative Procedure Act BE 2539 (1996), which determines the maximum administrative fine of not exceeding 20,000 baht per day unless a specific governing regulation stipulates otherwise. ²¹

In addition, the government authority that grants a licence to the juristic person to conduct a specific type of business may exercise its power to suspend or revoke the licence if the licensee does not comply with the law or the conditions prescribed in the licence. The result of this can be damaging and can potentially lead to a further criminal offence if the business continues to operate without a proper licence. Also, revocation of the licence may lead to debarment as it will disqualify a person from applying for a new licence in the future.

iii Compliance programmes

Recent developments in this area indicate a greater recognition of the importance of compliance programmes as a defence to or as a mitigating circumstance for criminal liability; nevertheless, the area remains largely untested.

In mid 2015, amendments to the Organic Act on Counter Corruption introduced new language in Section 123/5 imposing liability on a juristic person where the offender has committed an offence in the interests of that juristic person. Interestingly, this provision introduced into law the defence of having ‘appropriate internal control measures to prevent the commission of the offence’, which is a significant advance towards recognising the

---

¹⁹ According to the judgment of the Supreme Court No. 787-788/2506, the Supreme Court ruled that the criminal penalties that can be enforced against a corporate entity are limited to fines and the confiscation of property. However, there are also provisions in specific legislation that include the revocation of licences as a related penalty.


²¹ Section 58 of the Administrative Procedure Act BE 2539 (1996): The administrative order which stipulates the doing or omission of certain act, its violation or non-observance by the person who is subject to such administrative order provides that the official may exercise any of the following administrative enforcement measures: (1) the official who personally enters into the handling of the subject matter or designates other persons to act on his behalf in which case the person who is subject to such administrative order shall be reimbursed for the expenses and extra money at the rate of 25 per cent per annum of the said expenses; (2) there shall be paid the administrative penalty in reasonable amount, but such penalty shall not exceed twenty thousand Baht per day...
importance of internal corporate compliance measures. There is as yet no indication as to how the defence will be interpreted by the courts. The ‘Guidelines on Appropriate Internal Control Measures for Juristic Persons to Prevent Giving Property or Other Benefits to State Officials, Foreign Public Officials and Agents of Public International Organisations’ require juristic persons to have appropriate internal control measures in place that stipulate that companies should internally adopt measures to prevent bribery from the top-level management, conduct risk assessments, adopt measures for high-risk and vulnerable areas, carry out anti-bribery programmes for business partners and associated subsidiaries, keep accurate books and accounting record systems, human resource management policies for anti-bribery measures, report suspicions of bribery and conduct periodic evaluation of anti-bribery effectiveness. If a company has an appropriate ‘internal control’ in place, liability can be mitigated; however, internal control measures do not guarantee that juristic persons will not be liable as it depends on the enforcement of said measures.

iv Prosecution of individuals
Thai criminal law recognises the concept of ‘principals’, ‘instigators’ and ‘supporters’ of an offence. Under the provisions of the Criminal Code, two or more persons may be subject to the same penalty for an offence, while a supporter would be liable for two-thirds of the penalty.

For example, a private-sector entity or individual may become involved in an NACC investigation and any subsequent proceedings if the private party has allegedly participated in or aided in the commission of such offence, either as an instigator or supporter of the alleged violation and accused official, including where such person has provided some property or benefit to the political office holders or officials to induce them to act contrary to their duties. A recent example in which private entities or individuals were investigated and sued as co-defendants, with the accused officials, was the ‘fire truck scandal’, which involved the procurement of fire-fighting vehicles and equipment by the Bangkok Metropolitan Administration from a consortium. Another example is the Rubber Seed case, in which three private companies, a number of their respective directors and those authorised persons who signed key documentation, were sued as ‘supporters’ of the commission of the offence.

An employer is not required to dismiss an employee convicted of a criminal offence; however, if that employee is sentenced to imprisonment by a final court judgment, the employer may terminate employment without the requirement to pay statutory severance to the employee. It is generally the case that an employer may dismiss an employee, provided that all required statutory severance payments and notice provisions have been met, although

---

22 Section 123/5, Paragraph 2 of the Organic Act on Counter Corruption: If the offence under paragraph one is committed by any person related to any juristic person and the action is taken for the benefit of such juristic person, and the juristic person does not have in place appropriate internal control measures to prevent the commission of such offence, the juristic person shall be deemed to have committed the offence under this section and shall be subject to a fine of one to two times of the damages caused or benefits received.

23 The ‘Guidelines on Appropriate Internal Control Measures for Juristic Persons to Prevent Giving Property or Other Benefits to State Officials, Foreign Public Officials and Agents of Public International Organisations’, issued by the Office of the National Anti-Corruption Commission, came into effect on 16 December 2017.

24 Section 66 of the Organic Act on Counter Corruption: a principal, an instigator or a supporter, including a person who gives, asks to give or promises to give property or other benefits to the person under paragraph one [i.e., the official] with a view to inducing him to act or omit or delay an act resulting in a dishonest act in the performance of duties.
the employee may nevertheless choose to allege that the dismissal was unfair and seek payment of additional compensation.25 There are only limited circumstances in which an employer can terminate the employment without making the required severance payment to the employee.26

IV INTERNATIONAL

i Extraterritorial jurisdiction

According to the Criminal Code, Thailand recognises the territorial principle on a criminal offence that is either partially or wholly committed in Thailand, or has consequences in Thailand. Thailand has adopted the passive personality principle in 13 categories of offences aiming to protect public security, economic security, personal integrity and property.27

In addition, Thailand exercises the universal jurisdiction principle regarding crimes committed outside Thailand and specific offences that are considered threats to national and international security, or known as transnational crimes, such as human trafficking, terrorism financing, piracy, sexual offences, as well as corruption of government officials and money laundering as prescribed in the Criminal Code and certain specific legislation. For example, Section 6 of the Anti-Money Laundering Act provides the universal jurisdiction principle over any person who has committed a money laundering offence whether inside or outside Thailand.28

With respect to investigative powers, specific investigation authorities, such as the NACC and the Anti-Money Laundering Board, are empowered by their respective legislation to conduct investigations on offences committed outside Thailand.

ii International cooperation

Thailand cooperates with other countries according to both informal cooperation via diplomatic channels and formal cooperation as prescribed in international agreements or treaties. Thailand has entered into international agreements with certain countries on both civil and criminal matters.

With respect to civil matters, the Civil Procedure Code provides that a Thai court may request a foreign court to conduct civil proceedings on its behalf. At present, Thailand has entered into an agreement on judicial cooperation with six countries.

With respect to criminal matters, the Act on Mutual Assistance in Criminal Matters BE2535 (1992) provides that the government of Thailand, as coordinated by

25 Section 49 of the Act for the Establishment of and Procedure for Labour Court BE 2522 (1979): In the dismissal case, if the Labour Court considers the dismissal unfair, it shall order the employer to reinstate the employee at the same level of wage at the time of dismissal. However, if the Labour Court thinks that such employee and employer cannot work together, it shall fix the amount of compensation to be paid by the employer which the Labour Court shall take into consideration the age of the employee, the working period of the employee, the employee’s hardship when dismissed, the cause of dismissal and the compensation the employee is entitled to receive.


the Attorney-General’s Office, may request assistance from foreign states, and *vice versa*, regarding investigation, inquiry, prosecution, forfeiture of property and other proceedings relating to the criminal matters. At present, Thailand has entered into mutual legal assistance treaties with seven countries. The DSI recently used a mutual legal assistance treaty with the United States by requesting the investigation of a witness who resides in the United States. In this case, the US Department of Justice instructed the FBI to obtain testimony as per the DSI’s request. The testimony obtained from the FBI’s investigation was later admitted in a Thai court.

In addition, Thailand is a member of Interpol, which connects it to the global police information system, enabling the exchange of information on criminal conduct; however, the information so obtained would be subject to the investigation principle prescribed by the Criminal Procedure Code that the evidence derived by any unlawful means shall not be admitted in court.29 Thailand commonly cooperates and coordinates with other countries in the areas of trafficking in persons and people smuggling, child exploitation, drug trafficking, cybercrime, economic crime, terrorism, arms smuggling and intellectual property crime;30 for example, the co-investigation between Interpol and Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam on cybercrime.31 Another example is the strengthening of border security networks to prevent the movement of criminals and terror suspects within ASEAN.32 Thailand has also joined the Global Forum on Transparency and Exchange of Information for Tax Purpose to reach international standards of exchange of information to combat tax avoidance and tax evasion.33

At present, Thailand has entered into 11 extradition treaties covering 15 countries. According to the Treaty on Extradition, the contracting states are not obliged to extradite their own citizens to other states. Grounds of refusal are statute of limitations, lack of the same criminal offences, political offences, violation of right to a fair trial, insufficiency of evidence and double jeopardy.

### iii Local law considerations

In the case where multiple jurisdictions are implicated in an investigation, the local law in Thailand that may need to be taken into consideration is the data privacy law. The draft of the Personal Data Protection Act is expected to be submitted for Cabinet approval in May 2018 and enactment by the end of the year. The general concept of personal data protection can be found in various legislation, such as the Telecommunications Business Act BE 2544 (2001),

29 Section 226 of the Criminal Procedure Code: *Any material, documentary or oral evidence, likely to prove the guilt of the innocence of the accused, is admissible, provided it is not obtained through any inducement, promise, threat, deception or other unlawful means; such evidence shall be produced in accordance with the provisions of this Code or other laws governing production of evidence.*

30 Interpol, Mission and Crime priorities. Available at https://www.interpol.int/Member-countries/Asia-South-Pacific/Thailand.


32 'Interpol, training looks to enhance border security in Southeast Asia'. Available at www.interpol.int/News-and-media/News/2017/N2017-054.


For example, the Financial Institution Business Act BE 2551 (2008) provides that any business information obtained from a financial institution, such as a commercial banking business, is to be kept confidential except for the case of disclosure for investigation or proceedings conducted by the government authority.34 Additionally, Clause 11 of the Lawyers Council Regulation on Lawyer Conduct BE 2529 (1986) provides that lawyers with certified licences shall not disclose any confidential information about the client that has come into their possession in the course of performance of their duties as a lawyer unless approval has been obtained by the client or through a court order. Therefore, even though the concept of data privacy has been acknowledged in Thailand, the disclosure of this information for the purposes of investigation or court trial is an exception. However, the exception provided under these laws is not clear as to what extent an investigation conducted by an international investigation body or the investigation agency of other jurisdictions shall also be covered. In our view, international cooperation either through diplomatic channels or international agreements would be an option for a multiple-jurisdiction investigation.

V YEAR IN REVIEW

As reported in the 2017 Corruption Perceptions Index by Transparency International, Thailand is ranked at 96 of 180 countries with a score of 37 out of 100,35 which indicates that corruption remains an important issue.

In recent years, there have been some interesting cases relating to the investigation of alleged corruption in Thailand, for example the Rolls-Royce case, in which there is an accusation that Rolls-Royce made illicit payments over more than 20 years to officials in the Thai state-owned enterprises; the Krung Thai Bank case, in which the executives of the bank were sentenced to 18 years in prison by the Supreme Court for approving more than 9.9 billion baht in loans to one real estate developer company, even though the company was already listed with the bank as a non-performing debtor with non-performing loans; and the Rai Som case, in which a well-known TV host and managing director of Rai Som and the company’s financial officer were sentenced by the Appeal Court to imprisonment of 13 years four months for the embezzlement of advertising revenue from the Mass Communications Organisation of Thailand for supporting official malfeasance under Sections 6, 8 and 11 of the Act on Offences Committed by Officials of State Organs or Agencies BE 2502 (1959).

As shown by the recent amendment to the Organic Act on Counter Corruption, the existence of a strong internal compliance measure may provide a defence or factor mitigating the application of penalties. In addition, the NACC’s ‘Guidelines for Internal Control Measures in Preventing Bribery of Public Officials, Foreign Public Officials, and Agents of Public International Organisations,’ which became effective in December 2017, aim to assist juristic persons in establishing appropriate measures to prevent bribery and cultivate a culture of corporate governance in the private sector.

---

35 Thailand, Corruption Perceptions Index 2017. Available at www.transparency.org/country/THA.
VI CONCLUSIONS AND OUTLOOK

Regulatory authorities, such as the police and the DSI, and tax authorities such as the Revenue and Customs Departments and the local authorities, have extensive powers of search and seizure under Thai law. It is also common for raids to be conducted at the onset of government investigations; therefore, there is a need to prepare the relevant personnel for such a possibility.

It is advisable for a company to prepare a ‘telephone tree’ and assign an inspection coordinator, as well as replacements, if there is the risk of a raid. The inspection coordinator should be familiar with the action plan and act as the main contact when investigators arrive, which is usually without notice.

Investigators typically present a search warrant upon arrival at the premises and that search warrant will specify the time period for conducting the raid. Some laws allow searches without a warrant, but in practice a warrant is usually provided. While the phrase ‘dawn raid’ is often used, it is typically the case that a raid would be conducted during daylight hours or, even more commonly, during business hours. Investigators will generally ask for an authorised director of the company and may already have an affidavit of the company that contains these details, as such names are a matter of public record on file with the Department of Business Development of the Ministry of Commerce.

External legal counsel should be called to assist during the raid. It is preferable that officials be asked to wait until the arrival of the designated external lawyers, although there is no guarantee that they will do so. During the raid, each inspector should be accompanied at all times by an external or in-house lawyer or such person as has been designated by the company. In the event that an inspector has questions, the inspector should be asked to put their questions in writing. In the event that the inspectors request a company representative to sign notes or documents, the representative should only sign to acknowledge that a record was taken and a copy received on the relevant date, and not that the representative agrees with or accepts any information set out in the record.
INTRODUCTION

With a new US presidential administration has come a modest recalibration of enforcement priorities but there has been little evidence of a significant 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 are launched weekly, it seems. In the environmental law and consumer fraud arena, Volkswagen reached an agreement with regulators last year 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. Eight former VW executives and employees were criminally charged for their role in the conspiracy, one of whom was sentenced in December 2017 to seven years in prison; this is in keeping with the more aggressive stance by the Department of Justice (DOJ) in recent years in pursuing and obtaining guilty pleas from individuals implicated in corporate misconduct.

In the financial sector, regulators continue actively to investigate currency and interest rate manipulation, charging two former Société Générale employees with manipulating LIBOR to allow their employer to create a false impression of the creditworthiness of their employer, while a former executive of HSBC Bank plc was convicted for fraud involving the manipulation of foreign exchange markets. And 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.

On the foreign bribery front, after a pause in the announcement of new settlements after the presidential transition, enforcement resumed at a rapid pace with the DOJ and SEC bringing a combined 32 enforcement actions against entities and individuals in 2017, resulting in approximately US$1 billion in penalties. Dozens of companies are known to be under investigation for potential FCPA violations, and the DOJ reiterated its commitment to robust enforcement of anti-corruption laws in a widely publicised speech by Deputy Attorney General Rod Rosenstein. 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, last year’s record-setting Telia anti-corruption settlement, which resulted in the imposition of more than US$1 billion...
million in criminal fines, penalties and forfeiture to authorities in the United States and elsewhere, was the result of an investigation conducted jointly by authorities in the United States and the Netherlands, with significant assistance provided by authorities in Austria, Belgium, Cyprus, France, Ireland, Latvia, Luxembourg, Norway, Switzerland, the Isle of Man and the United Kingdom. Similarly, the recent US$800 million corruption settlement with Rolls-Royce to resolve bribery allegations relating to improper payments in Asia and South America was coordinated among US, UK and Brazilian authorities.

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 US Commodity Futures Trading Commission (CFTC), the US Departments of Commerce, Labor and the Treasury, the Federal Energy Regulatory Commission and the Occupational Safety and Health Administration. Many of these agencies are empowered to commence formal investigations and enforcement proceedings on their own initiative and impose monetary sanctions or other penalties, and these powers have expanded in recent years. For instance, in August 2010, the enforcement arm of the SEC was granted permanent authority to issue subpoenas for documents and witnesses and to compel testimony in connection with investigations into financial wrongdoing.

Still, the DOJ, which is 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 is 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, however, the DOJ frequently coordinates with other federal agencies, as well as state and local authorities. For example, the 2017 Volkswagen settlement resulted from an investigation that was closely coordinated between the DOJ and the EPA, and, in recent years, the DOJ has worked closely with the IRS’s Criminal Investigative Division to investigate and charge Swiss banks with facilitating tax fraud by US taxpayers, including obtaining an indictment in 2012 against a bank for allegedly hiding more than US$1.2 billion in secret accounts. That cooperation continued in 2013 with US and Swiss regulators rolling out a new programme that affords to Swiss banks implicated in tax evasion the opportunity to avoid formal prosecution by paying penalties and providing certain information about accounts held by US taxpayers. In early 2014, Credit Suisse pleaded guilty to charges of criminal tax evasion and was fined US$2.6 billion. Recently, the DOJ has expanded its tax evasion investigations to other jurisdictions, with enforcement actions related to banking activities in the Caribbean region, the Middle East and India.

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 ‘stripping’, or removing identifying information from payment messages on behalf of parties subject to US trade sanctions administered by the Office of Foreign Assets Control (OFAC)
of the US Treasury Department. In 2012, Standard Chartered paid US$340 million to the New York State Department of Financial Services and US$227 million to the DOJ, the New York County District Attorney’s Office and other federal regulators to resolve charges stemming from payments and trade business with sanctioned parties. HSBC paid a then-record US$1.9 billion in late 2012 for failures in its anti-money laundering programme and its own business with sanctioned parties; BNP Paribas paid an US$8.9 billion fine for similar conduct in 2014; and Commerzbank AG paid a total of US$1.45 billion in March 2015. Earlier this year, US Bancorp agreed to pay US$613 million in penalties to authorities for deficiencies in its anti-money laundering programme, which resulted in suspicious activity going unreported. The DOJ investigations in this regard have been conducted in conjunction with the New York County District Attorney’s Office, OFAC and the US bank regulatory agencies. Cooperation between federal agencies and state and local authorities has become more common, with various ‘task forces’ created to coordinate the agencies’ efforts; this includes the financial fraud enforcement task force, which was set up by the Obama administration and brings together representatives from various agencies and state and local authorities to take action against financial fraud, with a recent special focus on corporate entities engaged in mortgage fraud.

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 and regulatory 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 – even before conviction – 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. Notably, the US House of Representatives passed a bill in 2010 that would have made ‘debarment’ mandatory for an FCPA violation (though, ultimately, the bill was not passed by the US Senate). 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 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.

3 ABN AMRO, HSBC, ING Bank NV, Barclays, Credit Suisse, Lloyds TSB Bank, Standard Chartered, BNP Paribas and Commerzbank AG.
II CONDUCT

i Self-reporting

Most federal enforcement agencies 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 organization is officially notified of a criminal investigation’.

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 (1) comes forward to voluntarily disclose its participation, (2) makes restitution to victims of the cartel, and (3) 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 have made various other 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, however, 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

---

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.
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). Just a few months ago, the DOJ announced that it was informally expanding this policy outside the FCPA context.

Even with this additional guidance from the DOJ, however, it is not completely clear that voluntary reporting should be the default action of every company that discovers potentially unlawful conduct within its organisation; at the very least, the company should assess the probability of independent discovery of the potential misconduct by government authorities. It is important to note, however, that 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 and the proliferation of new laws and regulations favourable to whistle-blowers.

A corporation 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 obligated 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 is also prudent to make the disclosures to all potentially related agencies. This is to ensure that the company receives credit for self-reporting from each regulator that could potentially bring an enforcement action. For example, if a company believes that one of its subsidiaries may have made an improper payment to a foreign official and has decided to voluntarily disclose that information to the SEC, it should strongly consider also informing the DOJ, given how frequently the two regulators bring parallel enforcement actions under the FCPA and the likelihood that the SEC will pass on any information received, or make a formal referral, to the DOJ.

In determining whether to self-report, and to what extent to cooperate with a regulatory investigation, corporations and their employees also must 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 obstructing 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.

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 can also be a weakness if it is perceived by the government to undermine its 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, of course, if any members of the company’s legal department are implicated in the conduct under investigation.

With respect to the conduct of 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 interviewee should also be informed that any information imparted during the interview may be shared with government authorities.

Unless it has not previously made any disclosures to the government and uncovers nothing to merit any disclosure during the course of the internal investigation, a company typically will 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. A 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 indictment is not warranted or that the situation calls for reduced charges; for example, (1) by emphasising that senior management was not implicated in the wrongdoing and, therefore, the misconduct was not pervasive, (2) that the company has no history of criminal conduct, or (3) that the collateral consequences of prosecution 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. Until recently, 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 has revised its policy 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.

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 the Dodd–Frank Wall Street Reform and Consumer Protection Act, which came into effect in 2011 and authorises the payment of rewards of between 10 and 30 per cent of judgments over US$1 million by the SEC to whistle-blowers who alert the SEC to certain types of wrongdoing and that result in successful enforcement actions. 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 annual report to Congress on the programme at the end of 2017, the SEC has received more than 22,000 tips since it was introduced in 2011, and has paid several substantial bounties to whistle-blowers who have given information leading to successful prosecutions. For example, in 2014, the SEC paid more than US$30 million to a whistle-blower who provided information leading to a successful enforcement action – the largest award to date – and issued awards totalling nearly US$50 million in 2017, including several multimillion-dollar awards. Given this new regulatory regime, a company must now 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 2015, the SEC brought an enforcement action against KBR Inc in connection with the company’s practice of discouraging potential whistle-blowers by means of confidentiality agreements prohibiting the reporting of wrongdoing without the company’s permission, which the SEC alleged violated a Dodd–Frank regulation barring companies from impeding communication between whistle-blowers and the SEC. In connection with the settlement of that action, KBR agreed to end the practice and paid a fine of US$130,000. Last year, 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.

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, prosecutory 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. While some courts have limited the application of this doctrine in recent years, it 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.
In the past, most corporate criminal investigations have ended with the two sides entering into a deferred prosecution agreement (DPA) or non-prosecution agreement (NPA), though there has been a marked increase in guilty pleas to resolved DOJ actions in more recent years, as noted above. 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 (1) cooperate fully with the agency’s investigation and in any other investigation that may be ongoing, (2) accept responsibility for the wrongdoing at issue and (3) 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 and may lead to a reduced sentence 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:

a. management that is knowledgeable about and able to oversee the programme competently;

b. adequate staffing of the programme;

c. training for all employees in compliance standards and procedures;

d. procedures for monitoring and periodic auditing of the programme’s effectiveness;

e. a system for the anonymous reporting of compliance breaches;

f. consistent enforcement of the programme; and

g. 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 has 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, which until very recently was a common requirement of a DPA or NPA, but which was also a practice that had come under criticism for being unduly disruptive to the company and excessively remunerative to the monitors themselves. 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. However, there
was a resurgence of the imposition of outside monitors in 2016, with regulators imposing eight independent compliance monitors in connection with FCPA settlements. It is possible that this was a one-year aberration – no compliance monitors were imposed by the DOJ in FCPA corporate enforcement actions settled after the Trump administration in 2017, and the DOJ has announced that it will be undertaking a review of the monitor programme.

Notably, in their FCPA Resource Guide, the DOJ and the SEC reaffirmed the importance of the presence, or absence, of a robust compliance programme as a key factor in the regulators’ charging decision and in their determination of an appropriate settlement for a violation. The regulators cited a recent anti-corruption enforcement action against a Morgan Stanley employee, in which the SEC declined to charge the company itself in view of Morgan Stanley’s implementation of an extensive compliance system, as evidence of the SEC’s commitment to rewarding companies that put into place strong compliance programmes. The DOJ’s new corporate enforcement policy for FCPA actions also reaffirms the importance of implementing strong compliance polices and controls.

iv 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 recent years, the government has been 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’. The DOJ, under the new administration, has announced plans to review and potentially withdraw previously issued memos, including the Yates Memo, but this is unlikely to herald any diminished focus on individual prosecution, especially given numerous public comments by DOJ officials emphasising individual accountability for corporate crimes.

A discrete but related issue is the advancement or payment by a company under investigation of fees for attorneys for employees implicated in the wrongdoing at issue. While the DOJ’s stance until recent years, as with waiver of privilege, was that advancing such fees would weigh against a corporation in the DOJ’s cooperation determination, the government has now reversed that position, in part because of the ruling by the United
States Court of Appeals for the Second Circuit in *United States v. Stein*. In that case, the court upheld a trial court ruling that the DOJ had violated the Fifth and Sixth Amendment rights of certain KPMG employees when it communicated to KPMG that it would not look favourably upon the advancement of fees to employees incriminated in the accounting scandal for which KPMG was under investigation, despite KPMG’s historical practice of paying for its employees’ fees in such situations. At the same time as this decision, the DOJ announced that it would no longer consider advancement of fees as a factor influencing its cooperation determination, though it noted that the failure to terminate or adequately discipline employees would still be a consideration when making its indictment decision. Other agencies, such as the SEC, have not taken a clear stance with respect to this issue.

IV  INTERNATIONAL

i  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. This trend is evident in a variety of contexts. For example, in recent years the SEC has pursued a number of China-based issuers of US securities (as well as their auditors and accountants) for alleged financial fraud. Also, in the FCPA context, a significant number of enforcement actions during the past two 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 at times have 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. While a small number of court decisions 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.
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 UK’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 the 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, three recent nine-figure FCPA settlements were the result of cooperative investigations between US and foreign authorities.6

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 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.

6 These were the Keppel Offshore & Marine Ltd settlement, the Telia Company AB settlement, and the Rolls-Royce plc settlement.
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. Almost a year and half into the new presidential administration, there is 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 near-term softening of corporate enforcement is not on the cards. And while traditional areas of enforcement, such as anti-corruption, financial fraud, healthcare fraud and environmental protection, are likely to remain the mainstays of regulatory action, a number of other areas have emerged during the past year and are likely to receive substantially increased focus going forward. Most prominent among these is cybersecurity, which encompasses issues relating to data security, privacy and hacking, cryptocurrencies and related technologies, all of which present significant regulatory challenges. The SEC, for example, has already announced the formation of a ‘cyber unit’ targeting misconduct relating to abuse of financial markets through hacking, and has begun to turn its eye to potential cryptocurrency regulatory action through laws and regulations designed to protect investors. 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.
ABOUT THE AUTHORS

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 20 years and is an associate professor of criminal law and criminal procedure at the School of Law, 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 Committee of the Council of the Bars and Law Societies of Europe (chair, 2007 to 2013), the Criminal Law Experts Commission (Ministry of Justice) and FraudNet of the Commercial Crime Services of the International Chamber of Commerce.

VISITSAK ARUNSURATPAKDEE
R&T Asia (Thailand) Limited
Visitsak focuses his practice on regulatory compliance, mergers and acquisitions, capital markets, litigation, taxation and general corporate matters. He advises foreign and Thai multinational clients on regulatory compliance in their business operations and has represented them in various cases. Arising out of his work for energy and telecommunications companies in various M&A deals and concession-related disputes, Visitsak has also expanded his practice to include disputes with government agencies over the terms of concessions and administrative decision-making.
RYOTA ASAKURA
*Momo-o, Matsuo & Namba*

Ryota Asakura is an associate of Momo-o, Matsuo & Namba. Mr Asakura routinely represents clients in litigation concerning corporate malfeasance and has extensive experience in all aspects of internal investigations, especially as a member of an internal investigation committee. His corporate transactional practice is wide-ranging and includes mergers and acquisitions and, in particular, effective due diligence of acquisition targets.

Mr Asakura is also a specialist in 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.

PHIL BECKETT
*Alvarez & Marsal Disputes and Investigations, LLP*

Phil Beckett is a managing director with Alvarez & Marsal’s disputes and investigations practice in London and leads their European forensic technology capabilities. He brings more than 19 years of experience in forensic technology engagements, advising clients on forensic investigations of digital evidence, the interrogation of complex data sets, information governance, cyber and the disclosure of electronic documents. Mr Beckett was recently named again as the *Who’s Who Legal: Investigations* Digital Forensic Expert of the Year.

Mr Beckett has led anti-bribery investigations, kickback investigations, IP theft cases, employment disputes, fraud investigations, cartel and antitrust investigations and compliance review exercises, as well as supported commercial litigation and international arbitration. Many of these cases have been cross-border, requiring close monitoring of data protection and privacy legislation and the appropriate use of technology. These include a regulatory investigation for a global bank involving collecting, processing and hosting from multiple systems and jurisdictions, including instant-message chat and trading data.

Mr Beckett has regularly been appointed as an expert and managed the execution of multisite civil search orders whereby data has been captured and interrogated to meet court requirements. Mr Beckett was also instructed as an expert witness in *Imerman v. Tchenguiz* ([2010] EWCA Civ 908).

ALEXANDRE BISCH
*Debevoise & Plimpton LLP*

Alexandre Bisch is a senior associate 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.
JORGE BOFILL

Bofill Escobar Abogados

Jorge Bofill is an experienced dispute resolution attorney in the areas of white-collar crime, corporate investigations, civil litigation, international arbitration and mediation.

Mr Bofill is often requested as an expert by the Chilean Senate’s Committee on Constitution and Legislation. Examples of his involvement in these matters are the complete revamping of the Chilean criminal procedure system and the statute on criminal liability of legal entities, among many others. In April 2015, Mr Bofill was selected as a member of the panel of experts appointed by the Secretary General of the United Nations to conduct an assessment of the system of administration of justice of the United Nations.

Mr Bofill has been ranked in the top tiers in the fields of dispute resolution and white collar by Chambers Latin America since 2009, in 2015 received the distinction of ‘Star Individual’ in white-collar litigation.

He received his law degree from Pontifical Catholic University of Valparaíso, *summa cum laude*, and his doctoral degree from Friedrich-Alexander University Erlangen-Nürnberg, Germany, *summa cum laude*.

Mr Bofill is a professor of law at University of Chile School of Law and a board member of the Chilean Bar Association.

NICOLAS BOURTIN

Sullivan & Cromwell LLP

Nicolas Bourtin is a litigation partner at Sullivan & Cromwell LLP and the managing partner of the firm’s criminal defence and investigations group. His practice focuses on white-collar criminal defence and internal investigations, class-action defence, and securities and 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 University of Notre Dame and is a graduate of Columbia Law School, where he was a Harlan Fiske Stone scholar.

SUPRATIM CHAKRABORTY

Khaitan & Co LLP

Supratim Chakraborty is an associate partner of Khaitan & Co, LLP, Kolkata. He focuses his expertise on corporate and commercial transactions such as mergers, acquisitions, joint ventures and general corporate law advisory. He has advised several clients on various aspects of anti-bribery and anti-corruption law and has been part of several prominent M&A transactions, assisting domestic as well as foreign clients in structuring, drafting, negotiating and implementing complex deals. Supratim regularly advises clients on data protection and data privacy issues.
JASON CHAN  
*Allen & Gledhill LLP*

Jason is co-head of the firm’s white collar and 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.

Jason is recommended by *The Legal 500 Asia Pacific* for his expertise in dispute resolution, and is described as ‘highly eloquent’ and ‘extremely fast in sizing up any complex issues’. He has received numerous awards and commendations for outstanding advocacy. Jason previously served in the Singapore Legal Service as a deputy public prosecutor and state counsel, and was appointed as an assistant registrar of the Supreme Court.

Jason is a council member of the Law Society of Singapore and serves on its Complaints Committee and Inadequate Professional Services Complaints Committee. Jason also sits on the Accounting and Corporate Regulatory Authority’s Complaints and Disciplinary Panel. Jason serves as a member of several committees of the Singapore Academy of Law, including the Law Reform Committee.

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 Korea financial intelligence unit of the Financial Services Commission.

FREDERICK T DAVIS  
*Debevoise & Plimpton LLP*

Frederick T Davis is of counsel 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.

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 the then 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 offences against financial and socio-economic interests, fraud, criminal insolvency, misappropriation, misrepresentation and falsification of documents, corporate offences, bribery, 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 is currently ranked in Band 2 by Chambers Europe.

ULF DJURBERG
Setterwalls Advokatbyrå 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.

NICOLA DUNLEAVY
Matheson

Nicola Dunleavy is a partner in Matheson’s commercial litigation and dispute resolution department. She has a broad commercial litigation practice, with leading expertise in complex multi-jurisdictional disputes. Nicola heads Matheson’s arbitration team and is an experienced advocate in alternative dispute resolution. Her domestic and international clients are active in the pharmaceutical, chemicals, food and drink, waste, water, energy, mining and transport sectors. She represents clients in contract disputes, public procurement and competition litigation, judicial review and major development, environmental, planning and property disputes.

Nicola is an associate of the Irish Taxation Institute, an associate of the Chartered Institute of Arbitrators and a member of Energy Law Ireland and the Irish Environmental Law Association. She is a frequent speaker at conferences and workshops on regulatory enforcement and on commercial arbitration and litigation. She has authored contributions to a number of publications, including The International Comparative Legal Guide to International Arbitration from 2011 to 2016.
GAUTHAMA CARLOS COLAGRANDE FORNACIARI DE PAULA
Siqueira Castro Advogados

Gauthama C C Fornaciari de Paula is a partner in the criminal department of Siqueira Castro Advogados. He received a master of science in law and development at Fundação Getulio Vargas and a bachelor in law from the University of São Paulo.

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.

NATHANIEL GREEN
Sullivan & Cromwell LLP

Nathaniel Green is a special counsel at Sullivan & Cromwell LLP. He has experience in a broad range of matters, including internal and government agency investigations brought by the DOJ, SEC and other regulators, as well as securities, bankruptcy and antitrust litigation in state and federal court, and before arbitration tribunals. Mr Green received his undergraduate degree magna cum laude from Amherst College and is a graduate of Stanford Law School.

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 Korea. He is a Chambers Asia Leading Individual for Dispute Resolution (White-Collar Crime, 2015–2018), and was named an Expert for Investigations by Who’s Who Legal (2016–2017).

MARK HUGHES
Slaughter and May

Mark Hughes is a partner in Slaughter and May Hong Kong’s dispute resolution department. He joined Slaughter and May’s dispute resolution department in London in 2003, moving to the Hong Kong office in 2010. He has a broad practice that includes advising on regulatory investigations and inquiries, civil and commercial litigation in the Hong Kong High Court, the management of overseas litigation, arbitration under different international rules, and alternative dispute resolution mechanisms, including mediation.
PETER IBRAHIM
Steptoe & Johnson UK LLP
Peter Ibrahim is an associate in Steptoe & Johnson’s London office and a member of the international regulation and compliance and FCPA and anti-corruption groups. He has assisted with internal investigations of potential breaches of company compliance policies or law as well as the defence of investigations by regulators and enforcement agencies. His experience includes providing clients with compliance counselling and conducting due diligence on third parties.

ANDRIS IVANOVS
Steptoe & Johnson UK LLP
Andris Ivanovs is an associate in Steptoe & Johnson’s London office and is a member of the firm’s international regulation and compliance, and FCPA and anti-corruption groups. He advises clients on compliance with anti-corruption and anti-bribery laws, including the UK Bribery Act and the US Foreign Corrupt Practices Act, anti-money laundering laws, as well as sanctions and export and trade controls. Andris also defends companies and individuals facing white-collar crime investigations and regulatory enforcement actions brought by the UK and US authorities.

VINAY JOY
Khaitan & Co
Vinay Joy is a partner in the corporate and white-collar practice group and is based at the firm’s Bengaluru office. Vinay has considerable experience in advising companies and their promoters in carrying out internal investigations, conducting workshops on being prepared against dawn raids by various statutory authorities, and on matters concerning allegations of fraud and wrongdoing. Vinay also advises clients on various issues concerning white-collar crime, including aspects of ethics and anti-corruption policies, whistle-blower protection, complaint mechanisms and domestic enquiries against unethical conduct and corrupt practices.

Vinay specialises in advising a wide variety of clients on merger and acquisition transactions, joint ventures, private equity and venture capital transactions, due diligence exercises and contractual matters. He is also part of the firm’s labour and employment law practice and specialises in all aspects of non-contentious employment law matters, including those arising as a consequence of business transfers, integration of acquired businesses and internal compliance audits.

ALEX KIM
Shin & Kim
Tong Kun (Alex) Kim is a foreign attorney at Shin & Kim and his major practice areas include government investigations, cross-border mergers and acquisitions, and general corporate advice. Mr Kim joined Shin & Kim in 2015 upon obtaining his juris doctorate at Berkeley School of Law, University of California. Mr Kim is a member of the State Bar of California.
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, as well as complex litigation, in France.

TOMASZ KONOPKA
Sołtysiński Kawecki & Szeląg
Tomasz Konopka joined Sołtysiński Kawecki & Szeląg in 2002, and has been a partner since January 2013. Tomasz specialises in business-related criminal cases, including white-collar crime, investigations, representation of clients related to custom seizures of counterfeit products, cybercrimes and court litigation. He represents Polish and foreign clients before the courts and law enforcement authorities. He currently leads the criminal law department. Prior to joining Sołtysiński Kawecki & Szeląg, Tomasz was a lawyer in a number of companies, including those listed on the Warsaw Stock Exchange. He is also a member of the Association of Certified Fraud Examiners.

VICTOR LABATE
Siqueira Castro Advogados
Victor Labate is associate in the criminal department of Siqueira Castro Advogados. He holds a bachelor of law degree from University of São Paulo (USP). Victor has also participated on an exchange programme with the Erasmus Universiteit Rotterdam, Netherlands, to study criminology. For that, he received an academic merit scholarship from USP.

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, including The Legal 500 Asia Pacific. He is cited as a ‘leading individual’ and described as ‘one of the market leaders’, ‘responsive and reliable’ and ‘highly experienced’, ‘understands commercial issues’ and for providing ‘robust, thorough and sound advice’.

Vincent is presently an adjunct faculty member of the School of Law of the Singapore Management University (since 2011) and Singapore Institute of Legal Education (since 2004). He was previously an adjunct faculty member of the Faculty of Law of the National University of Singapore (2004 to 2013). Vincent has been involved in various law reform reports, has published articles in various law journals and has contributed chapters to numerous leading practitioner texts, including the Singapore Civil Procedure 2018, Bullen & Leake & Jacob’s Singapore Precedents of Pleadings (2016), and Halsbury’s Laws of Singapore: Volume 4: Civil Procedure (2016).
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.

VANESSA McALLISTER

wkk law Rechtsanwälte

Vanessa McAllister has been an associate at wkk law Rechtsanwälte since October 2016. Vanessa mainly assists Norbert Wess in corruption and white-collar crime cases. She graduated from University of Salzburg in 2013 and worked as a research assistant in the Department of Criminal Law of 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 specialised publications.

CLAIRE McLoughlin

Matheson

Claire McLoughlin is a partner in Matheson’s commercial litigation and dispute resolution department. She advises a wide variety of clients on contentious matters, including in relation to corporate offences. Claire has particular expertise in relation to investigations relating to fraud and financial crime.
MARKUS MACHAN

*wkk law Rechtsanwälte*

Markus Machan has been an associate at wkk law Rechtsanwälte since February 2015. Markus mainly assists Norbert Wess in corruption and white-collar crime cases. He graduated from University of Vienna in 2009 and worked as a research assistant in the Department of Criminal Law of 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 University of Vienna and St Pölten University of Applied Sciences, a member of the Association of Austrian Defence Lawyers (VÖStV) and author of numerous specialised publications.

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 (then) 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).

ANAND MEHTA

*Khaitan & Co*

Anand Mehta is a partner in the corporate and M&A and white-collar practice group and is based at the firm’s Mumbai office. Before joining Khaitan & Co, Anand was a partner at Thakker & Thakker for 10 years and now has more than 25 years of experience. Anand specialises in mergers and acquisitions, India entry strategies, corporate, commercial and contract laws. Over the years, Anand has assisted several clients, including some Fortune 500 companies, to establish and expand their India operations, including forming joint ventures and other strategic alliances. His forte, apart from mergers and acquisitions, includes employment, data privacy and protection and preventive work on white-collar crime matters.
ALEX MELIA  
*Steptoe & Johnson UK LLP*

Alex Melia is an international counsel in Steptoe & Johnson’s London office and a member of the international regulation and compliance, and FCPA and anti-corruption groups. Her practice is focused on assisting companies in conducting internal investigations involving bribery, money laundering and other regulatory compliance issues. She has conducted numerous investigations for clients across a wide range of industries and geographies.

Ms Melia also defends companies and individuals facing investigations and enforcement actions brought by the UK’s Serious Fraud Office, Financial Conduct Authority and other law enforcement and regulatory agencies.

Ms Melia has significant experience in leading compliance audits and risk assessments and helping clients develop effective anti-corruption and anti-money laundering compliance strategies. She also has considerable experience in advising clients on the design, implementation and evaluation of global compliance programmes.

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.

KAKUJI MITANI  
*Momo-o, Matsuo & Namba*

Kakuji Mitani is a partner of Momo-o, Matsuo & Namba. Mr Mitani’s main area of practice comprises general corporate law matters, including compliance and white-collar crime. He has broad experience in antitrust and competition law. Mr Mitani has represented numerous companies and individuals investigated or accused by the US Department of Justice and other competition authorities in a wide range of international cartel cases. He regularly advises clients on multi-jurisdictional leniency applications. Mr Mitani’s extensive antitrust and competition law experience includes representing and defending clients in investigations before the Japan Fair Trade Commission and providing advice on preventive and compliance measures. His expertise includes the field of marketing and advertising compliance. Mr Mitani also handles complex commercial litigation and international arbitration cases.

Mr Mitani received his LLB from The University of Tokyo, Faculty of Law in 2000 and was admitted to the Japanese Bar in 2002. He obtained his LLM from Columbia Law School in 2007 and was admitted to the New York Bar in 2008.
JACOB MØLLER DIRKSEN

_Horten Law Firm_

Jacob Møller Dirksen specialises in complex commercial litigation and arbitration and is head of Horten’s commercial disputes and arbitration practice group and the firm’s insurance and liability sector team. He has wide experience in commercial dispute resolution and conducts cases before the courts and both Danish and international arbitration tribunals. He is often appointed as arbitrator, including in cases under the auspices of the Danish Institute of Arbitration and the International Chamber of Commerce. Jacob Møller Dirksen advises primarily in cases concerning contractual liability, mergers and acquisitions disputes, agency and distribution agreements, directors’, auditors’ and attorneys’ liability, construction, commercial and product liability, financial sector disputes and insurance law.

In addition to being admitted to the Danish Bar, Jacob Møller Dirksen has studied in England and Australia (LLM). Throughout his career as an attorney, he has extensively assisted in international cases and therefore has a distinct international approach to and comprehension of advising on cross-border issues.

SOFIE OTTOSSON

_Setterwalls Advokatbyrå AB_

Sofie Ottosson 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. Sofie has extensive experience in anti-corruption work and internal investigations within the private and public sectors.

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 forensic accounting group’s contentious insolvency specialism and has worked alongside insolvency practitioners in a number of roles: as expert accountant, adviser, undertaking investigations to follow cash, and tracing and recovering assets.
DANIEL PRAETORIUS

*Bofill Escobar Abogados*

Daniel Praetorius focuses on securities, regulatory and white-collar crime litigation.

He has broad experience representing clients in criminal cases related to business activities and anti-corruption regulations as well as in securities enforcement proceedings. He has also been involved in the development of compliance programmes and has conducted internal corporate investigations.

For many years, Mr Praetorius also practised as a corporate attorney, advising clients on corporate, mergers and acquisitions and finance matters, experience that usefully complements his litigation skills on complex economic disputes.

He previously worked at Bofill Mir & Álvarez Jana, Morales & Besa, the Chilean National Prosecutor’s Office’s Money Laundering, Business and Organised Crime Special Unit and at Freshfields Bruckhaus Deringer LLP in Frankfurt, Germany.

Mr Praetorius received his law degree (JD equivalent) from Universidad de Chile, *summa cum laude*. He obtained his LLM degree, *summa cum laude*, at Albert Ludwig University of Freiburg, Germany, studies that were sponsored by the ALBAN programme of high-level scholarships for Latin American students implemented by the European Commission.


SUSMIT PUSHKAR

*Khaitan & Co*

Susmit Pushkar is a partner in the dispute resolution practice group and is based at the firm’s New Delhi office. Susmit has diverse and rich experience in advising clients across industries and laws. He regularly appears before the trial courts, the High Courts and the Supreme Court of India.

Susmit advises corporate houses in relation to investigations by government agencies (e.g., Serious Fraud Investigation Office, Central Bureau of Investigation, Enforcement Directorate, Economic Offence Wing) alleging bribery, money laundering, corporate fraud and various other offences, and represents clients through trial in criminal courts and appellate proceedings. He assists clients in their internal corporate investigations relating to corporate fraud, whistle-blowing and harassment. Susmit is part of the competition practice group of the firm and advises clients in relation to competition litigation, including cartel and abuse of dominance.

Susmit regularly handles high-stake and complex litigation involving multiple stakeholders and regulatory bodies. During the past 14 years, Susmit has represented clients across several industries in their commercial, corporate, shareholders and other disputes before courts and arbitral tribunals, including international commercial arbitrations (e.g., ICC, SIAC, LCIA, GAFTA). He has led several constitutional challenges of legislations before the writ courts. Susmit brings considerable and valuable multidimensional experience in his areas of practice.

*Chambers & Partners* highlights Susmit as being ‘increasingly recognised in the market for “some stellar work” in the dispute resolution and white-collar crime spaces’. He has been nominated for the role of vice chairman for the Inter-Pacific Bar Association Committee on Anti-Corruption and the Rule of Law for 2018–2020. He regularly speaks in seminars on legal issues affecting the industry.

© 2018 Law Business Research Ltd
JOÃO DANIEL RASSI  
_Siqueira Castro Advogados_

João Daniel Rassi is the head partner of the criminal department of Siqueira Castro Advogados. He holds a specialisation in criminal law at Salamanca University, Spain, has received a master’s degree in criminal law from University of São Paulo (USP) and has a doctorate in both criminal law and criminal procedure law from USP.

Throughout more than 20 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 the environment, 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 Brazilian Office of Prosecutor General.

Mr Rassi has been listed by *Chambers and Partners*, *Latin Lawyers* 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.

KAREN REYNOLDS  
_Mattheson_

Karen Reynolds is a partner in Matheson’s commercial litigation and dispute resolution department. She is regularly instructed in relation to complex contentious regulatory matters. Karen has particular expertise in the insurance and financial services sectors.

JOHN RUPP  
_Steptoe & Johnson UK LLP_

John Rupp is a partner in Steptoe & Johnson’s London office and is a member of the international regulation and compliance and FCPA and anti-corruption groups. His acumen in matters relating to anti-corruption compliance and internal investigations has been recognised repeatedly by both *Chambers UK* and *The Legal 500 UK*.

Mr Rupp’s practice focuses on structuring and undertaking internal investigations involving trade controls, bribery, money laundering and accounting issues. He also routinely interacts with senior enforcement officials in multiple jurisdictions on bribery and money laundering matters.

Mr Rupp has extensive experience in providing FCPA and UK Bribery Act advice and assisting companies in revising their compliance policies and procedures. He also has served as coordinating counsel in commercial disputes arising simultaneously in several countries.

Mr Rupp has served for many years on the editorial board of the *Global Investigations Review*. He also is a frequent speaker at international compliance conferences.
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 and commercial department and the competition and antitrust practice.

A pioneering competition law specialist in Singapore and ASEAN with unparalleled antitrust experience in South East 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 approximately 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 in the second one, and has defended parties in 100 per cent of Singapore’s international cartel decisions to date.

Daren has also worked on several landmark abuse of dominance cases, 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.

MELISA UREMOVIC  
*R&T Asia (Thailand) Limited*

Melisa has more than 18 years’ experience working in Thailand. She has a particular expertise in trade and customs matters, and complex regulatory matters involving tax, competition, anti-bribery, foreign ownership and data protection, focusing on both compliance and investigations. She is recognised in *Who’s Who Legal: Trade & Customs* 2017 and 2018 for Thailand and is a recommended lawyer for dispute resolution in *The Legal 500 Asia Pacific 2017*.

KEVIN WARBURTON  
*Slaughter and May*

Kevin Warburton is a counsel in Slaughter and May Hong Kong’s dispute resolution 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.
NORBERT WESS

wkk law Rechtsanwälte

Norbert Wess is a founder and partner at wkk law Rechtsanwälte. He graduated from 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 Dr Wess 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 Zeitschrift für Wirtschafts- und Finanzstrafrecht (journal for business and tax criminal law) and of the Handbuch Strafverteidigung (2017).

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

CMS von Erlach Poncet Ltd

Aline Wey Speirs is a counsel at CMS. 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.

GAVIN WILLIAMSON

BDO LLP

Gavin is a partner in BDO’s UK forensic practice based in London. He is a chartered accountant and certified fraud examiner, specialising exclusively in forensic accounting investigations on behalf of corporate and institutional clients. His practice ranges from the investigation of white-collar crime, financial fraud, theft and bribery, to wider forms of employee and institutional misconduct such as confidentiality breaches and conflicts of interest.

Although Gavin is based in London, he works extensively overseas. He has conducted major investigations in Switzerland, Spain, Turkey, Ireland, the Middle East and North Africa, eastern Europe, and central and east Asia. Gavin has supported organisations in a wide range of industry sectors, from not-for-profit to retail, and from energy and resources to construction, property and manufacturing. Gavin has also worked extensively for clients in the financial services sector – insurance companies, hedge funds, banks and sovereign wealth funds. His financial services experience encompasses sanctions, anti-money laundering and fraud investigations. He has reported to US prosecutors and law enforcement agencies on behalf of banks and other organisations.
Gavin has a special interest in the use of technology in the investigation of fraud and corruption and of asset tracing. He has presented widely on innovations in forensic technology and their practical application to investigation and disclosure.

Gavin has an honours degree from Queen’s University of Belfast and a doctorate from University of Dundee, both in civil engineering. He is a fellow of the Institute of Accountants in England and Wales and a member of the Fraud Advisory Panel.

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 20 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 University of Milan since 2003 and is president of the criminology master’s degree at University Carlo Cattaneo. Professor Zanchetti is the author of more than 50 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 considerable experience in cases of corporate compliance, money laundering and cross-border criminal proceedings. She is very actively involved in internal corporate investigations and risk management assessment for national and multinational corporations.
CONTRIBUTING LAW FIRMS’ CONTACT DETAILS

**ALLEN & GLEDHILL LLP**
One Marina Boulevard, 28-00
Singapore 018989
Tel: +65 6890 7188
Fax: +65 6327 3800
jason.chan@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
Fax: +44 20 7487 3686
stephen.peters@bdo.co.uk
gavin.williamson@bdo.co.uk
www.bdo.co.uk

**ALVAREZ & MARSAL DISPUTES AND INVESTIGATIONS, LLP**
One Finsbury Circus
London
EC2M 7EB
United Kingdom
Tel: +44 20 7663 0778
Fax: +44 20 7715 5201
pbeckett@alvarezandmarsal.com
www.alvarezandmarsal.co.uk

**BOFILL ESCOBAR ABOGADOS**
Avenue Apoquindo 3472
19th floor, Patio Foster Building
7550105 Las Condes
Santiago
Chile
Tel: +562 2483 9000
jbofill@bofillescobar.cl
dpraetorius@bofillescobar.cl
www.bofillescobar.cl

**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

**CMS VON ERLACH PONCET LTD**
Dreikönigstrasse 7
PO Box 8022
Zurich
Switzerland
Tel: +41 44 285 11 11
Fax: +41 44 285 11 22
bernhard.loetscher@cms-vep.com
aline.wey@cms-vep.com
cms.law
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
akirry@debevoise.com
ftdavis@debevoise.com
abisch@debevoise.com
www.debevoise.com

DE PEDRAZA 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@depedrazaabogados.com
paula.mbarros@depedrazaabogados.com
www.depedraza.com

HORTEN LAW FIRM
Philip Heymans Allé 7
2900 Hellerup
Copenhagen
Denmark
Tel: +45 33 34 40 00
Fax: +45 33 34 40 01
jmd@horten.dk
www.horten.dk

KHAITAN & CO
Simal
2nd Floor
7/1 Ulsoor Road
Bengaluru 560 042
India
Tel: +91 80 4339 7000
Fax: +91 80 2559 7452
vinay.joy@khaitanco.com

Emerald House
1B Old Post Office Street
Kolkata 700 001
India
Tel: +91 33 2248 7000
Fax: +91 33 2248 7656
supratim.chakraborty@khaitanco.com

One Indiabulls Centre
13th Floor, Tower 1
841 Senapati Bapat Marg
Mumbai 400 013
India
Tel: +91 22 6636 5000
Fax: +91 22 6636 5050
anand.mehta@khaitanco.com

Ashoka Estate
12th Floor
24 Barakhamba Road
New Delhi 110 001
India
Tel: +91 11 4151 5454
Fax: +91 11 4151 5318
susmit.pushkar@khaitanco.com

whitecollar@khaitanco.com
www.khaitanco.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
www.linklaters.com
Contributing Law Firms' Contact Details

MATHESON
70 Sir John Rogerson’s Quay
Dublin 2
Ireland
Tel: +353 1 232 2000
Fax: +353 1 232 3333
nicola.dunleavy@matheson.com
claire.mcloughlin@matheson.com
karen.reynolds@matheson.com
www.matheson.com

MOMO-O, MATSUO & NAMBA
Kojimachi Diamond Building 6F
4-1 Kojimachi, Chiyoda-Ku
Tokyo 102-0083
Japan
Tel: +81 3 3288 2080
Fax: +81 3 3288 2081
ryota.asakura@mmn-law.gr.jp
mitani@mmn-law.gr.jp
www.mmn-law.gr.jp

NYMAN GIBSON MIRALIS
Level 9, 299 Elizabeth Street
Sydney
NSW 2000
Australia
Tel: +61 2 9264 8884
Fax: +61 2 9264 9797
pg@ngm.com.au
dm@ngm.com.au
https://ngm.com.au

R&T ASIA (THAILAND) LIMITED
973 President Tower, 12th Floor
Units 12A–12F, Ploenchit Road
Lumpini, Pathumwan
Bangkok 10330
Thailand
Tel: +66 2 656 1991
Fax: +66 2 656 0833
visitsak.a@rajahtann.com
melisa.u@rajahtann.com
https://th.rajahtannasia.com

SHIN & KIM
8th Floor, State Tower Namsan
100 Toegye-ro, Jung-gu
Seoul 04631
Korea
Tel: +82 2 316 4114
Fax: +82 2 756 6226
sjinchoi@shinkim.com
tkhong@shinkim.com
akim@shinkim.com
www.shinkim.com

SIQUEIREIRA CASTRO ADVOGADOS
Rua Tabapuá, No. 81, 4th Floor
Itaim Bibi
São Paulo 04533-010
Brazil
Tel: +55 11 3704 9840 / 3594 0900
Fax: +55 11 3704 9848
rassi@siqueiracastro.com.br
gfornaciari@siqueiracastro.com.br
vlabate@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
mark.hughes@slaughterandmay.com
kevin.warburton@slaughterandmay.com
www.slaughterandmay.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
sofie.ottosson@setterwalls.se
www.setterwalls.se
<table>
<thead>
<tr>
<th>Firm Name</th>
<th>Address 1</th>
<th>City</th>
<th>Country</th>
<th>Tel:</th>
<th>Fax:</th>
<th>Email 1</th>
<th>Email 2</th>
<th>Email 3</th>
<th>Email 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SOŁTYSIŃSKI KAWECKI &amp; SZLĘZAK</strong></td>
<td>ul. Jasna 26</td>
<td>00-054 Warsaw</td>
<td>Poland</td>
<td>+48 22 608 70 00</td>
<td>+48 22 608 70 70</td>
<td><a href="mailto:tomasz.konopka@skslegal.pl">tomasz.konopka@skslegal.pl</a></td>
<td><a href="http://www.skslegal.pl">www.skslegal.pl</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STUDIO LEGALE</strong></td>
<td>Via Bianca di Savoia, 9</td>
<td>20122 Milan</td>
<td>Italy</td>
<td>+39 2 4548 5700</td>
<td>+39 2 4548 5701</td>
<td><a href="mailto:m.zanchetti@studiolegalepz.it">m.zanchetti@studiolegalepz.it</a></td>
<td><a href="mailto:info@studiolegalepz.it">info@studiolegalepz.it</a></td>
<td><a href="http://www.studiolegalepz.it">www.studiolegalepz.it</a></td>
<td></td>
</tr>
<tr>
<td><strong>STUDIO LEGALE PULITANÒ-ZANCHETTI</strong></td>
<td>Via Bianca di Savoia, 9</td>
<td>20122 Milan</td>
<td>Italy</td>
<td>+39 2 4548 5700</td>
<td>+39 2 4548 5701</td>
<td><a href="mailto:m.zanchetti@studiolegalepz.it">m.zanchetti@studiolegalepz.it</a></td>
<td><a href="mailto:info@studiolegalepz.it">info@studiolegalepz.it</a></td>
<td><a href="http://www.studiolegalepz.it">www.studiolegalepz.it</a></td>
<td></td>
</tr>
<tr>
<td><strong>STUDIO LEGALE</strong></td>
<td>Via Bianca di Savoia, 9</td>
<td>20122 Milan</td>
<td>Italy</td>
<td>+39 2 4548 5700</td>
<td>+39 2 4548 5701</td>
<td><a href="mailto:m.zanchetti@studiolegalepz.it">m.zanchetti@studiolegalepz.it</a></td>
<td><a href="mailto:info@studiolegalepz.it">info@studiolegalepz.it</a></td>
<td><a href="http://www.studiolegalepz.it">www.studiolegalepz.it</a></td>
<td></td>
</tr>
<tr>
<td><strong>STEPTOE &amp; JOHNSON UK LLP</strong></td>
<td>5 Aldermanbury Square</td>
<td>London</td>
<td>United Kingdom</td>
<td>+44 20 7367 8000</td>
<td>+44 20 7367 8001</td>
<td><a href="mailto:pibrahim@steptoe.com">pibrahim@steptoe.com</a></td>
<td><a href="mailto:aivanovs@steptoe.com">aivanovs@steptoe.com</a></td>
<td><a href="mailto:amelia@steptoe.com">amelia@steptoe.com</a></td>
<td><a href="mailto:jrupp@steptoe.com">jrupp@steptoe.com</a></td>
</tr>
<tr>
<td><strong>SULLIVAN &amp; CROMWELL LLP</strong></td>
<td>125 Broad Street</td>
<td>New York</td>
<td>United States</td>
<td>+1 212 558 4000</td>
<td>+1 212 558 3588</td>
<td><a href="mailto:bourtin@sullcrom.com">bourtin@sullcrom.com</a></td>
<td><a href="mailto:green@sullcrom.com">green@sullcrom.com</a></td>
<td><a href="http://www.sullcrom.com">www.sullcrom.com</a></td>
<td></td>
</tr>
<tr>
<td><strong>WKK LAW RECHTSANWÄLTE</strong></td>
<td>Himmelpfortgasse 20/2</td>
<td>1010 Vienna</td>
<td>Austria</td>
<td>+43 1 532 13 00</td>
<td>+43 1 532 13 00 90</td>
<td><a href="mailto:n.wess@wkklaw.at">n.wess@wkklaw.at</a></td>
<td><a href="mailto:m.machan@wkklaw.at">m.machan@wkklaw.at</a></td>
<td><a href="mailto:v.mcallister@wkklaw.at">v.mcallister@wkklaw.at</a></td>
<td><a href="http://www.wkklaw.at">www.wkklaw.at</a></td>
</tr>
</tbody>
</table>

© 2018 Law Business Research Ltd