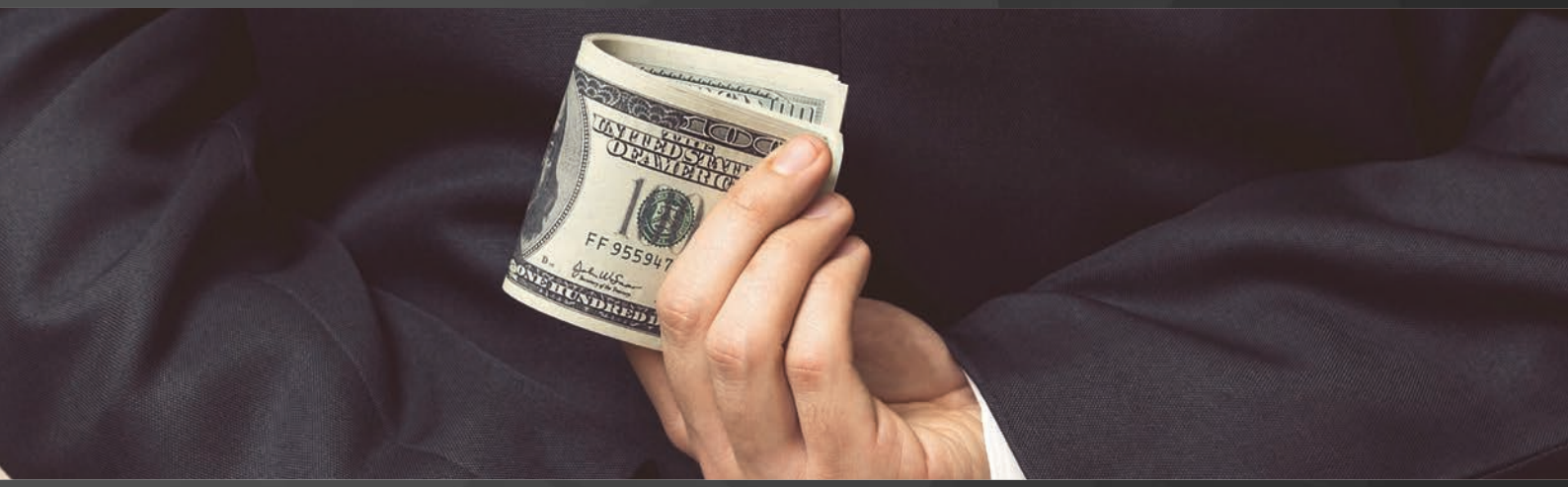
International Comparative Legal Guides



Business Crime 2020

A practical cross-border insight into business crime

10th Edition

Featuring contributions from:

Advokatfirma DLA Piper Norway DA
AGS Legal
Anagnostopoulos
AO2 Law
Atsumi & Sakai
BDO LLP
Clayton Utz
CMS Rodríguez-Azuero
Debevoise & Plimpton LLP
Del Rosal & Adame
Drew & Napier LLC
Durrieu Abogados
ENACHE PIRTEA & Associates S.p.a.r.l.
Haldanes
Hamdan Al Shamsi Lawyers and Legal Consultants
Homburger
Joyce Roysen Advogados
Kachwaha and Partners
Lawfirm Holzhacker
Lee and Li, Attorneys-at-Law
Matheson
Morais Leitão, Galvão Teles, Soares da Silva & Associados, S.P. R.L.
Noerr s.r.o.
Peters & Peters LLP
Rahman Ravelli
Sjöcrona Van Stigt
Skadden, Arps, Slate, Meagher & Flom LLP
Skrine
Sołtysiński Kawecki & Szlęzak
Studio Legale Pisano

ICLG.com

ISBN 978-1-83918-000-2
ISSN 2043-9199

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 0720
www.iclg.com

Group Publisher
Rory Smith

Publisher
Jon Martin

Sales Director
Florjan Osmani

Senior Editors
Caroline Oakley
Rachel Williams

Creative Director
Fraser Allan

Chairman
Alan Falach

Printed by
Ashford Colour Press Ltd.

Cover Image
www.istockphoto.com

Strategic Partners

Business Crime 2020

10th Edition

Contributing Editors:
Keith Krakaur and Ryan Junck
Skadden, Arps, Slate, Meagher & Flom LLP

Expert Chapters

Country Q&A Chapters

Recent Trends in U.S. Enforcement and the Advent of Technology Legislation


Ryan Junck


Pippa Hyde

Skadden, Arps, Slate, Meagher & Flom LLP

As global markets have become more interconnected and complex, business crime is, more than ever, an area involving intricate schemes often across multiple jurisdictions. As a result, enforcement bodies have had to upgrade their investigatory methods to keep pace with the field. This chapter examines recent trends and provides an update on recent U.S. and international technology legislation that will affect the global business crime enforcement space. It addresses several trends in U.S. enforcement and U.S. and European legislation governing the handling and transfer of data, including policies aimed at encouraging companies to self-report, increased cooperation among international regulators and relatively recent technology legislation.

Self-Reporting

The U.S. Department of Justice (DOJ), the U.S. Commodities Futures Trading Commission (CFTC), and the U.S. Securities and Exchange Commission (SEC) have all emphasised the benefits of corporations self-reporting wrongdoing and cooperating with the U.S. government. At the end of 2017, the DOJ formally incorporated its cooperation policy for corruption cases into the U.S. Attorneys' Manual. According to this policy, the presumption is that the DOJ will decline to prosecute a company for violations of the Foreign Corrupt Practices Act (FCPA) where a company (i) voluntarily self-discloses the alleged misconduct, (ii) fully cooperates with the DOJ, and (iii) timely and appropriately remediates the situation. Where the DOJ does pursue an enforcement action, under this policy, if a company has complied with these three criteria, the DOJ will recommend a 50 percent reduction from the low end of the U.S. sentencing guidelines fine range. Even if a company does not self-disclose, but still fully cooperates and remediates, it can earn a 25 percent fine reduction. In 2018, the DOJ declined to prosecute in 11 of 13 cases where a company had voluntarily self-disclosed, and the remaining two were resolved with non-prosecution agreements.

Similarly, the CFTC published guidance in 2017 highlighting the benefits of self-reporting, estimating that parties could receive a 50–75 percent reduction in penalties assessed if they self-report and cooperate. In September 2017, James McDonald, the Director of Enforcement at the CFTC, noted that the CFTC may decline to prosecute in "extraordinary circumstances", such as "where misconduct is pervasive across an industry and the company or individual is the first to self-report".

Lastly, the SEC has a policy that lists self-reporting among the factors for the SEC to consider in granting leniency to a company and has shown in practice that companies can receive leniency for cooperation. Indeed, during a speech in May 2018, SEC Enforcement Division Co-Director Steven Peikin noted that the SEC would continue to "provide incentives to those who come forward and provide valuable information" to the SEC. For example, in February 2019, Gladius Network LLC, as a part of its settlement with the SEC relating to violations of U.S. securities laws for improperly marketing a cryptocurrency, evaded a civil monetary penalty from the SEC as a result of self-reporting and cooperation.

DOJ Policy Against "Piling On"

In an effort to encourage companies to self-disclose misconduct, the DOJ has signaled its desire to make business crime enforcement more efficient by limiting the number of agencies that investigate and punish companies for the same underlying misconduct, a practice referred to as "piling on". This policy was officially announced and incorporated into the U.S. Attorneys' Manual in May 2018, and it encourages DOJ attorneys to coordinate with other authorities to eliminate "the unnecessary imposition of duplicative fines, penalties and/or forfeiture against the company".

In the U.S., this policy seeks to reduce the likelihood that multiple enforcement bodies investigate and penalise companies for misconduct, meting out punishments that are not proportionate to the alleged misconduct. It is increasingly typical that the DOJ and the SEC work cooperatively to investigate related corporate misconduct and coordinate their settlements and penalties.

This policy is also having an impact on settlements involving multiple authorities outside the U.S. For example, in the 2018 settlement with Petrobras, the Brazilian state-owned oil company plagued with bribery allegations, Petrobras paid the bulk of its $850 million penalty to Brazilian authorities, while the U.S. authorities took 10 percent of the penalty.

Moreover, other U.S. authorities may be following the DOJ's lead on this policy. In a March 2019 CFTC announcement that the agency would henceforth be pursuing foreign bribery cases, an area usually dominated by the SEC and the DOJ, Mr. McDonald made clear that the CFTC's enforcement would not "pile onto other existing investigations" and that any penalty leveled by the CFTC would account "for any imposed by any other enforcement body".

International Cooperation in Enforcement

In a similar fashion, the DOJ has also emphasised the importance of international cooperation in investigations and settlements involving misconduct that touches multiple jurisdictions. The DOJ pursues many non-U.S. companies and financial institutions, especially in its efforts to combat foreign corruption. In fact, as of March 2019, nine out of the 10 largest corruption penalties of all time involving a DOJ settlement have been with non-U.S. companies. This, combined with the anticorruption laws and enforcement bodies established in many countries worldwide, makes for a crowded enforcement space in complex international cases and necessitates international cooperation. One noteworthy example of this is the 2018 Société Générale settlement, which involved unparalleled coordination between the French Parquet National Financier and the DOJ, as the two authorities coordinated their settlements and agreed on a cumulative penalty. Other notable

examples include the Rolls-Royce settlement in 2017, which involved coordination and fee-sharing among U.S., U.K. and Brazilian authorities, and the Odebrecht and Braskem settlements in 2016, which involved coordination among U.S., Brazilian and Swiss authorities in determining and sharing penalties.

The Role and Reach of Technology Law

Recent legislation regarding data sharing also reinforces the trend of enhanced international coordination.

In the U.S., the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act), enacted in 2018, has two distinct components. First, it enables federal law enforcement to compel providers of "electronic communication services" and "remote computing services" to disclose data in their "possession, custody, or control" even where that data is located outside of the U.S. Second, it authorises the U.S. government to enter into executive agreements with foreign governments to facilitate cross-border exchanges of data. These agreements also allow non-U.S. law enforcement agencies to request electronic data directly from U.S. companies. Companies served with a subpoena or warrant can challenge it on the bases that (i) the user whose data is sought is not a U.S. person or does not reside in the U.S., or (ii) disclosure would materially risk violation of the laws of a foreign government. The U.S. nexus requirement is broad and could include a communications services provider using the U.S. banking system, having business or operation in the U.S. or use of email with a server situated in the U.S.

The CLOUD Act constitutes a significant tool for both U.S. and non-U.S. authorities in seeking out data that is held outside of their jurisdictions. The new law offers another method for authorities to seek data held in overseas jurisdictions outside of the mutual legal assistance treaty (MLAT) process, which is often criticised as being overly burdensome and time-consuming. Negotiations are ongoing between the U.S., EU and U.K. to create such executive agreements that would allow U.S. authorities to demand data held in the EU and the U.K., and for EU and U.K. authorities to demand data held in the U.S.

The CLOUD Act also may be the start of a trend of similar laws. Less than a year after it became law in the U.S., the U.K. enacted the Crime (Overseas Production Orders) Bill (COPO), in February 2019, which allows U.K. judges to compel parties overseas to produce electronic data if there is an international agreement in place between the U.K. and the country in question. The recipient of an overseas production order is served directly and has a default period of seven days in which to produce the required data, which is highly compressed for the scale of typical cross-border investigations. As COPO does not grant U.K. courts any punitive power, failure to comply with an order may, at worst, result in a contempt of court proceeding. Thus, while COPO, like its U.S. counterpart, seeks to side-step the time and cost issues associated with the MLAT process, its reliance on courts to enforce production orders and seven-day production requirements may signal that the practical effect of COPO on large-scale cross-border investigations could prove to be minor.

In any case, given the evolving legal landscape governing the production of data, companies need to consider carefully where and with what cloud service providers they store their data, as a strategy of simply placing a server in a particular country may no longer be enough to protect the data from the long arm of the law.

While the CLOUD Act may serve as an extra tool for U.S. authorities, the E.U. General Data Protection Regulation 2016/679 (the GDPR) reaffirmed, and in certain instances narrowed, the legal bases on which personal data can be processed and subsequently transferred outside of the European Economic Area (the EEA). Although not the first data privacy law to regulate personal data in the EEA, the GDPR has caught the attention of companies with its largest potential fines set at 4 percent of annual global turnover or €20 million, whichever is greater. In the specific realm of business crime, the GDPR presents a number of challenges related to how investigations are conducted and how data, which will inevitably include personal data, can be produced to regulatory or enforcement bodies outside of the EEA.

The GDPR may affect the conduct of internal investigations and the communication of responses to regulatory or enforcement authority inquiries by placing obligations on companies required to collect and review data containing personal data. The first step for any company when considering whether to process the personal data of custodians is to determine whether they have been provided with adequate prior notice of the processing activity envisaged, and whether they have been properly informed in this notice of a miscellany of other important information, such as what their rights are and, where applicable, the fact that their personal data may be transferred outside of the jurisdiction. The next step is to assess whether the company has a legal basis for processing the personal data in question.

In the context of employee data, companies may wish to rely on the consent of employees to collect and review their data; however, regulatory guidance on consent indicates that, given that there is a perceived imbalance of power in the employment context, it is doubtful that valid consent could be obtained from employees. If not based on consent, the collection and review may be based on a legitimate interest pursued by the company (or a third party); although, if relying on the legitimate interests legal ground to process employee data, the company takes on the extra responsibility for considering and protecting employees' rights and interests, among other requirements. In any event, and in all circumstances, when processing personal data, companies are required to abide by the GDPR's core principles. One of the core principles – data minimisation – requires that only personal data that is adequate, relevant and necessary for the purpose of the processing activity is processed.

Moreover, the GDPR imposes a restriction on the transfer of personal data outside the EEA to countries that the European Commission has not deemed to have adequate safeguards in place to protect personal data ("third-party countries"). This restriction can pose significant hurdles for business crime professionals who are working across jurisdictions and are obliged to provide information or to disclose personal data to regulators or enforcement authorities in third-party countries. One way to address this issue is to completely and permanently anonymise any personal data in submissions, effectively eliminating the transfer of "personal data" by stripping any identifiable information from the disclosure. However, there is a risk that by going down this route, a company may: (i) fail to achieve the extremely high bar of effecting a GDPR-compliant anonymisation of personal data; (ii) jeopardise disclosure obligations to foreign authorities; or (iii) find it more difficult to obtain cooperation credit from authorities.

Article 48 does allow for the transfer of personal data requested by a court, tribunal, or administrative authority of a third-party country outside the EEA, but only if it is based on an international agreement such as an MLAT between the two countries. Otherwise, Article 49 lists several other circumstances in which transfers to a third-party country may be permissible, but only in the absence of all other appropriate safeguards and where the transfer is occasional. These circumstances include where an employee explicitly consents to the transfer, or where the transfer is deemed necessary for the purposes of a contractual obligation, for important reasons of public interest, or for the establishment, exercise, or defence of legal claims.

Although tech giants such as Google and Facebook are facing GDPR enforcement investigations and ongoing actions, there have not been significant enforcement actions or legal disputes thus far involving business crime issues, such as transferring data to third-party countries pursuant to disclosure obligations or collecting

employee data as a part of an investigation. Nevertheless, the GDPR's accountability principle dictates that companies should carefully record all steps they take to comply with the GDPR in case a data protection authority makes an inquiry.

Conclusion

The business crime space in the U.S. and worldwide continues to be dynamic and evolving. For U.S. enforcement, prominent trends include policies aimed at promoting corporate self-disclosure, and increasing international and domestic cooperation. Both in the U.S. and internationally, the evolution of technology and the advent of new legislation that regulates its use and transfer is sure to continue – a trend that will create ongoing challenges for business crime professionals.

Acknowledgment

The authors would like to acknowledge the assistance of their colleague Alexander Hassanzadeh in the preparation of this chapter.

Ryan Junck is a partner in Skadden's European Government Enforcement and White Collar Crime Group. Mr. Junck represents corporations and individuals in criminal and civil matters in U.S. federal and state courts. He also has significant experience representing clients in U.S. and multi-national regulatory investigations, including those brought by the Department of Justice, the Securities and Exchange Commission, state attorneys general, district attorneys, the Office of Foreign Assets Control (OFAC), the Federal Reserve, the U.S. Congress and various international regulators. Mr. Junck has conducted numerous internal investigations and has substantial experience representing clients in cross-border matters, including investigations concerning insider trading, financial fraud, the Foreign Corrupt Practices Act (FCPA) and the economic sanctions laws administered by OFAC. He has represented clients and conducted investigations in various international jurisdictions, including China, France, Israel, Japan, Kazakhstan, Russia, Singapore, Switzerland, the United Arab Emirates and the United Kingdom.

Skadden, Arps, Slate, Meagher & Flom LLP
40 Bank Street, Canary Wharf
London E14 5DS
United Kingdom

Tel: +44 20 7519 7006
Email: ryan.junck@skadden.com
URL: www.skadden.com

Pippa Hyde is an associate in Skadden's European Government Enforcement and White Collar Crime Group. Her practice focuses on multinational investigations, representing individuals and companies in white collar criminal defence as well as civil and regulatory investigations. Ms. Hyde's experience includes advising clients on allegations relating to the FCPA, the U.K. Bribery Act, violations of economic sanctions and insider trading. Qualified in both the U.K. and U.S., Ms. Hyde worked for several years at Slaughter and May prior to joining Skadden.

Skadden, Arps, Slate, Meagher & Flom LLP
40 Bank Street, Canary Wharf
London E14 5DS
United Kingdom

Tel: +44 20 7519 7193
Email: pippa.hyde@skadden.com
URL: www.skadden.com

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Law
Business Crime
Cartels & Leniency
Class and Group Actions
Competition Litigation
Construction & Engineering Law
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Securitisation
Shipping Law
Telecoms, Media and Internet Laws
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by global legal group