GIR

EUROPE, MIDDLE EAST AND AFRICA

INVESTIGATIONS REVIEW 2022

Europe, Middle East and Africa Investigations Review 2022

Reproduced with permission from Law Business Research Ltd
This article was first published in May 2022
For further information please contact insight@globalinvestigationsreview.com

Published in the United Kingdom
by Global Investigations Review
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL

www.globalinvestigationsreview.com

To subscribe please contact subscriptions@globalinvestigationsreview.com

ISBN: 978-1-83862-869-7

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Preface

Welcome to the *Europe, Middle East and Africa Investigations Review 2022*, a Global Investigations Review special report.

Global Investigations Review is the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing - telling them all they need to know about everything that matters.

Throughout the year, the GIR editorial team delivers daily news, surveys and features; organises the liveliest events ('GIR Live'); and provides our readers with innovative tools and know-how products (such as the Enforcement Scorecard, the FCPA counsel tracker and the FCPA enforcement official database). In addition, assisted by external contributors, we curate a range of comprehensive regional reviews – online and in print – that go deeper into developments than the exigencies of journalism allow.

The *Europe, Middle East and Africa Investigations Review 2022*, which you are reading, is part of that series. It contains insight and thought leadership from 30 preeminent practitioners around these regions.

All contributors are vetted for their standing and knowledge before being invited to take part. Together they capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. The result is a book that's an invaluable horizon scanning tool.

This edition covers France, Italy, Romania, Russia, Switzerland, Central Europe, the United Kingdom, and the Gulf Cooperation Council (GCC) region, and has overviews on, among other things anti-money laundering.

As so often with these annual reviews, a close read yields many gems. On this occasion for this reader, they included that:

- the year 2021 saw a dip in global anti-money laundering activity, the first in a few years (but Europe bucked the trend);
- a political appetite that was growing in France to revivify the blocking statute seems to have waned – for now;
- the modernisation of insolvency law around the GCC is leading to more internal investigations across the Middle East. Individuals who no longer fear personal prosecution in the event of certain discoveries feel more able to dig into the root of their businesses' problems; and
- you can't argue that evidence is 'the fruit of the poisoned tree' in Switzerland!

We hope you enjoy the volume. If you have any suggestions for future editions, or want to take part in this annual project, we would love to hear from you. Please write to insight@globalinvestigationsreview.com

Finally, readers will notice two Russian chapters in this edition. For the avoidance of doubt, both were submitted before the war with Ukraine started. Our thoughts are with all those it has affected, particularly our Ukrainian friends and colleagues.

Global Investigations Review
London
May 2022

Anti-Money Laundering Trends and Challenges

Charlie Steele, Bhavin Shah, Gerben Schreurs, Sarah Wrigley and Deborah Luskin
Forensic Risk Alliance

IN SUMMARY

Despite a global decrease in 2021 in AML enforcement actions and penalties, they more than tripled in the Europe, the Middle East and Africa (EMEA) region from the year before. A few EMEA countries maintained momentum in regulatory activity, and the extraterritorial reach of the United States continued. Financial institutions and companies must respond to the continued strengthening of AML enforcement in the region, considering the related challenge of the extensive global sanctions imposed on Russia following the commencement of the war in Ukraine and the resulting movement of capital from Russia into EMEA and beyond.

DISCUSSION POINTS

- Changing legislative environment in key jurisdictions
- Recent AML typology trends
- Push towards AML effectiveness and what it means for regulators and financial institutions
- Key elements that should be present in a robust AML programme

REFERENCED IN THIS ARTICLE

- EU anti-money laundering directives
- UK Economic Crime Plan
- Recent US AML rules
- FATF mutual evaluation report on the UAE
- Virtual currencies, digital identity and AML typologies
- Public–private and private–private information-sharing partnerships
- FFIEC's key elements to an AML programme

Introduction

Enforcement actions and penalties for non-compliance with anti-money laundering (AML) regulations decreased sharply in 2021, reversing the upward trend of the past few years. This is most likely a temporary reprieve arising from regulators' efforts being hampered by the pandemic.

Global penalties totalled US$5.35 billion in 2021, compared with US$10.6 billion in 2020.[1] Despite this global decrease, Europe, the Middle East and Africa (EMEA) moved in the opposite direction, with a large increase in financial penalties at US$3.4 billion across the region – up from US$1 billion in 2020.

The increase can be traced to a few EMEA countries maintaining momentum in their regulatory activity in 2021, notwithstanding the disruption of the pandemic, as well as the continuing extraterritorial reach of the United States. French regulators issued the highest value enforcement action in the region against UBS for US$2 billion, followed by the United Kingdom (US$688 million), the Netherlands (US$577 million) and Bahrain (US$50.5 million). In addition, US regulators levied a penalty against UAE-based Mashreq for US$100 million.

Financial institutions and companies across EMEA need to plan their responses to the continued strengthening of AML enforcement, considering the related challenge of the unprecedented and extensive global sanctions imposed on Russia following the outbreak of the war in Ukraine and the resulting movement of capital out of Russia into Europe, Dubai and the rest of the world.

This article describes the changing legislative environment and recent typological trends. In addition, we highlight the push towards AML effectiveness and what that means for regulators and financial institutions. Finally, we outline the key elements that should be present in a robust AML programme.

Regulatory changes

European Union

There have been significant advances in money laundering legislation within the European Union, albeit with varying levels of implementation. A series of Anti-Money Laundering Directives (AMLDs) were passed between 1991 and 2021, the most recent of which include the Fifth AMLD (5AMLD) and the proposed Sixth AMLD (6AMLD).

Some of the more prominent additions within 5AMLD included:

1 Press release, 'Global Financial Institution Penalties on the Decline', *Fenergo* (6 January 2022).

- extending AML rules to additional providers, such as virtual currency exchange service providers and dealers in high-value goods;
- reducing anonymous prepaid card limits to €150;
- banning cards issued outside the European Union unless comparable AML regimes are in place in the jurisdiction of issue;
- making ultimate beneficial owner (UBO) lists public within 18 months;
- mandating functional public politically exposed persons (PEP) lists; and
- mandating enhanced due diligence measures to monitor transactions with high-risk countries.

There have been two layers of inconsistency in AML efforts within the European Union. First, AMLDs must be transposed into national law; however, the timeliness of that transposition has been patchy. For example, in February 2020, the European Commission sent letters of formal notice to eight EU countries for not having notified any implementation measures for the 5AMLD, which was updated more than two years prior and had a January 2020 deadline.[2] Even more concerning, in 2021, the European Commission sent letters of notice to Germany, Portugal and Romania for incorrectly transposing the Fourth AMLD (4AMLD), which had a transposition deadline of June 2017.[3]

Second, there have been a series of AML rule breaches in European banks that have raised doubts about the effectiveness of some of the member state supervisors. In some recent AML scandals, country supervisors only took action after the US Financial Crimes Enforcement Network (FinCEN) took special measures[4] or investigative journalists uncovered wrongdoing.[5]

---

2 Ruby Hinchliffe, 'European Commission warns eight countries over late AML laws', *Fintech Futures* (17 February 2020). The eight countries were Cyprus, Hungary, the Netherlands, Portugal, Romania, Slovakia, Slovenia and Spain.

3 European Commission, 'February infringements package: key decisions' (18 February 2021).

4 Frances Coppola, 'Why the U.S. Treasury Killed a Latvian Bank,' *Forbes* (28 February 2018).

5 'Swedish TV says Swedbank linked to Baltic money laundering scandal,' *Reuters* (20 February 2019).

The European Banking Authority (EBA) published a report which evaluated the effectiveness of member state AML supervision where they identified several areas of supervisory weakness, including not assessing control effectiveness versus confirming a prescriptive set of requirements, not taking proportionate and sufficient dissuasive measures, and not working effectively with domestic and international stakeholders.[6]

In July 2021, the European Commission made four AML proposals that promised to address some of the inconsistencies in AML regulations across the European Union.[7] The first proposal was to implement the new EU AML Authority.[8]

The second proposal was a new regulation for AML and combatting the financing of terrorism, transferring some rules related to customer due diligence and beneficial ownership from a directive, which requires transposition into national law, into a regulation, which is a binding legislative act.[9] This proposal also includes establishing an EU-wide limit of €10,000 for large cash payments and expands obliged entities to include cryptoasset service providers, crowdfunding platforms and migration operators.

The third proposal was the 6AMLD, which replaces the previous directive and includes provisions related to national supervisors and financial intelligence units (FIUs).[10] The previous legislation,[11] which harmonised 22 predicate offences across the European Union and extended criminal liability to legal persons, is now viewed as a legislative update in between the 5AMLD and the newly proposed 6AMLD.

The fourth proposal was related to expanding the traceability of cryptoasset transfers via the travel rule.[12]

United Kingdom

The United Kingdom is no longer required to implement EU AMLDs; however, it is likely that it will continue to match, or exceed, the AML rules set by the European Union.

---

6 European Banking Authority, 'EBA Report on Competent Authorities' Approaches to the Anti-Money Laundering and Countering the Financing of Terrorism Supervision of Banks' (5 February 2020).

7 European Commission, 'Anti-money laundering and countering the financing of terrorism legislative package' (20 July 2021).

8 Document 52021PC042.

9 Document 52021PC0420.

10 Document 52021PC0423.

11 Directive (EU) 2018/1673.

12 Document 52021PC0422.

The primary AML legislation in the United Kingdom is set out in the Proceeds of Crime Act 2002; the Terrorist Act 2000; the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017; and the Money Laundering Regulations 2019. A review of AML legislation is currently being carried out as part of the Economic Crime Plan 2019 to 2022, with proposals related to information sharing, the suspicious transaction reports (STRs) regime and AML effectiveness.[13]

A new Economic Crime Bill, thought to have been shelved in January 2022, was quickly drafted and enacted into law on 15 March 2022, following the commencement of the war in Ukraine.[14] Among other changes, the Economic Crime (Transparency and Enforcement) Act 2022 proposes a register for overseas ownership of UK property, making it easier for law enforcement to identify assets held by, for example, sanctioned Russian oligarchs. Under the current system, complex ownership structures, including opaque offshore entities, can be used to obscure true beneficial ownership.

The United Kingdom continues to be active in AML enforcement. The first criminal prosecution of a bank, NatWest, for money laundering concluded in late 2021 with a guilty plea and a penalty of £264 million.[15] The Financial Conduct Authority also levied a penalty of £64 million against HSBC for failings in its AML transaction monitoring systems.[16]

In February 2022, HM Revenue and Customs was the first UK law enforcement agency to seize three non-fungible tokens (NFTs) as part of an investigation into a suspected tax fraud.[17] The three digital artwork NFTs were seized along with other cryptoassets worth approximately £5,000.

United States

The primary legislation in the United States governing AML has grown over time from the Bank Secrecy Act of 1970 (BSA) to the Money Laundering Control Act of 1986, sections within the Patriot Act of 2001 and, most recently, the Anti-Money Laundering Act of 2020 (AMLA). There have also been smaller updates, such as the inclusion of virtual currency providers in 2013 and the Customer Due Diligence Rule requiring verification of customers in 2016.

---

13 EUSI, Economic Crime Plan Online Tracker.

14 GOV.UK, 'New measures to tackle corrupt elites and dirty money become law' (15 March 2022).

15 Financial Conduct Authority (FCA) press release, 'NatWest fined £264.8 million for anti-money laundering failures' (13 December 2021).

16 FCA, Decision Notice 2021: HSBC Bank plc.

17 'HMRC seizes NFT for first time in £1.4m fraud case', BBC (13 February 2022).

At the end of 2020, the United States passed a series of acts with significant improvements to the AML rules. Some of those new rules, such as a national beneficial owner registry and whistle-blower protections, bring the United States in line with existing EU rules.

In contrast, there are some rules that exceed those in the European Union and that may affect EU entities. The increased penalties enacted under AMLA are one example. They include prohibitions on knowingly concealing or misrepresenting a material fact from or to a financial institution concerning ownership or control of assets for PEPs or misrepresenting a material fact concerning the source of funds in a transaction that involves an entity that is a primary money laundering concern.[18] The penalties for violating these rules are up to 10 years' imprisonment or a US$1 million fine, or both.

Another example is the increased authority to subpoena documents from non-US financial institutions. Previously, these subpoenas could be issued to any non-US bank that maintained a correspondent account in the United States for records related to the specific correspondent account. The new statute expands this authority to allow the US Department of Justice (DOJ) to seek 'any records relating to the correspondent account or any account at the foreign bank, including records maintained outside of the United States' if the records are the subject of an investigation that relates to a violation of the BSA, a violation of US criminal laws, a civil forfeiture action or a primary money laundering concern investigation (as applied to ABLV Bank in Latvia in 2018).

Essentially, the subpoena powers have expanded from the specific correspondent account to any account at the non-US bank if they fall within one of those investigative categories. If the non-US financial institution fails to comply, the Act authorises the US Treasury to direct the related US financial institution to terminate the correspondent banking relationship, and it can also impose penalties.[19]

United Arab Emirates

The United Arab Emirates (UAE) has taken a number of steps in recent years to improve the AML and counter-terrorist financing (AML/CTF) landscape. Money Laundering was first criminalised in Federal Law No.4 of 2002, now replaced by Federal Law No. 20 of 2018, which provides the fundamental legislative framework that criminalises money laundering and terror financing. In addition, there is a national

18 Section 5335 of the Anti-Money Laundering Act of 2020 (AMLA).

19 Section 6308 of the AMLA 2020.

AML/CTF strategy and action plan that aims to ensure the effective implementation, supervision and continuous improvement of a national framework for the combatting of money laundering and terrorist financing.

Following a mutual evaluation report in 2020, the Financial Action Task Force (FATF) said that 'fundamental and major improvements' were still required by the UAE to avoid being placed on the FATF grey list.[20] The country is a major regional and international finance centre, has a significant gold market, extensive foreign property ownership and a sizeable cash-based economy, all of which place the country at high risk for money laundering and terror financing.

In March 2022, the FATF added the UAE to its grey list, which identifies jurisdictions deemed deficient but working with the FATF to improve.[21] The FATF said the UAE has committed to combatting sanctions evasion, increasing resources to use financial intelligence to combat money laundering and demonstrating a sustained increase in investigations and prosecutions of those activities. It further stated that the UAE has 'made a high-level political commitment' to strengthen the effectiveness of its regime, and over the past two years 'has made significant progress . . . to improve its system.'[22]

Virtual currencies

In October 2018, the FATF modified its recommendations to clarify that they apply to virtual assets and that virtual asset service providers should be regulated, licensed or registered, and subject to effective systems for monitoring or supervision. In June 2019, the FATF issued guidance with specific points for regulating digital assets and associated exchanges.[23]

The 5AMLD already requires virtual asset firms and exchanges to apply AML measures, including enhanced know-your-customer (KYC) programmes and reporting obligations. In November 2021, the European Council adopted the Regulation on Markets in Crypto Assets (MiCA), which aims to create a single licensing regime across all EU member states and streamline virtual asset regulation in the European Union for currently out-of-scope crypto-asset types, such as stablecoins and crypto-asset

20 Countries on the grey list are those found to have strategic AML deficiencies and will be subject to increased monitoring.

21 FATF, 'Outcomes FATF Plenary, 2-4 March 2022'.

22 Stephen Kalin and Rory Jones, 'U.A.E. Placed on Global Watch List for Money Laundering, Terrorism Financing', *The Wall Street Journal* (4 March 2022).

23 FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

service providers (a term that encompasses more service types). In practice, once a crypto firm is licensed in one EU member state, it can set itself up in other member states without obtaining an additional licence or approval from the local country.

The European Council and the European Parliament are now entering negotiations on the proposal. Most observers expect that the proposal will likely be passed in 2022 and take effect in 2024. Companies in the crypto space welcome the opportunity to operate in all EU countries with less red tape but have also noted that the legislation does not address decentralised finance, which is becoming an increasingly large and important part of the crypto space.

US regulators have been active in enforcement actions against crypto companies. Between 2009 and mid-2021, US regulators imposed US$2.5 billion in penalties relating to crypto assets. The largest portion was from the US Securities and Exchange Commission, but FinCEN levied US$183 million in that time frame.[24]

A few recent examples from FinCEN include a US$100-million civil penalty against BitMEX, a virtual currency derivatives exchange, in November 2021 for failing to implement an AML compliance programme and report certain suspicious activity.[25] Another example is the US$60-million penalty against the operator of virtual currency exchangers Helix and Coin Ninja in October 2020 for failing to register as a money service business, maintain an AML programme and report certain suspicious activity, particularly dark net market transactions.[26]

While the estimate of global money laundering of fiat currency is between US$800 billion and US$2 trillion every year, in comparison it is estimated that money laundering via cryptocurrency is approximately US$33 billion for the entire five-year period between 2017 and 2021.[27] As the use of cryptocurrencies increases, it is important to understand how to combat money laundering for this type of asset but also be aware that it is currently still a relatively small portion of the total value of money laundering that occurs each year.

---

24 Tom Robinson, 'Crypto Enforcement Actions by US Regulators Reach $2.5 Billion', *Elliptic* (21 June 2021).

25 *In the Matter of HDR Global Trading Limited, 100x Holdings Limited, ABS Global Trading Limited, Shine Effort Inc Limited, HDR Global Services (Bermuda) Limited d/b/a BITMEX*, No. 2021-02.

26 *In the Matter of Larry Dean Harmon d/b/a Helix*, No. 2020-2.

27 Chainalysis Team, 'DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate', Chainalysis (26 January 2022).

In addition, owing to the transparent nature of transactions recorded on the blockchain, the prospects for asset forfeiture appear more promising for cryptocurrencies. For example, IRS Criminal Investigation announced that it seized over US$3.5-billion worth of cryptocurrency in 2021, and the DOJ seized US$56 million in a scam investigation plus US$2.3 million from the ransomware group behind the Colonial Pipeline attack.[28]

AML challenges

Identifying UBOs

A critical component in combatting money laundering, and a regulatory expectation, is understanding who the customer is, who the UBOs are and the nature of their business. Determining the UBOs can be notoriously difficult when customers provide false information or use corporate vehicles in secrecy havens. It is timely and costly for compliance personnel to attempt to verify customer-provided UBO information.

Until 2020, most countries did not publish free, public ownership registers, so the information provided to financial institutions was more difficult to verify. Even when these lists are made available, such as with the UK Companies House, the information provided is not consistently verified.[29, 30]

The 5AMLD mandates publicly accessible UBO registers; however, many EU member states have either not established the registers or not made them publicly available.[31,32] In February 2021, Transparency International led a group of 700 signatories calling on the UN General Assembly to set standards for transparency of beneficial ownership; more specifically, it asked all countries to establish public registers of companies with the names of UBOs.[33]

---

28 The Chainalysis 2022 Crypto Crime Report (February 2022).

29 Oliver Bullough, 'How Britain can help you get away with stealing millions: a five-step guide', *The Guardian* (5 July 2019).

30 Pat Sweet, 'Companies House regime faces major overhaul', *Accountancy Daily* (7 May 2019).

31 'Patchy progress in setting up beneficial ownership registers in the EU', *Global Witness* (20 March 2020).

32 '404 Beneficial Owner Not Found: Are EU Public Registers in Place & Really Public?', *Transparency International* (26 May 2021).

33 'Hundreds of Academics, Civil Society Groups and Business Leaders Join Call for UN General Assembly to End Anonymous Shell Companies', *Transparency International* (24 February 2021).

Leveraging technology

There is a regulatory expectation that institutions monitor customer activity to identify suspicious patterns or behaviour. This can only be achieved when an institution effectively aggregates its data across systems, divisions and geographic locations; however, transactional data is often held in different repositories (eg, card services and deposit operations) and in numerous legacy systems owing to previous acquisitions. If the disparate data could be analysed as a group, it would likely improve the ability to identify potentially unusual transactional activity.

AML detection is often automated, but generally not predictive. If a machine learning (ML) solution was used to analyse the totality of customer and transactional data, entities could begin to identify unusual patterns that are worth investigating before they become known red flags.

Regulators have been encouraging innovative approaches, such as artificial intelligence (AI) and ML to more effectively identify suspicious activity. A joint statement issued by various US regulators in December 2018 encouraged the use of internal financial intelligence units devoted to identifying complex illicit finance threats and experiementing with AI and digital identity technologies.[34]

Utilising digital identity

Two key drivers in digital identity are becoming more prominent: the first is that of the estimated 2 billion unbanked adults worldwide, 360 million are unable to access the formal financial sector owing to insufficient identity documentation.[35] The second is that non-cash transactions are increasing,[36] and this trend is expected to continue.[37]

Digital identity has the potential to provide a high level of assurance regarding identification while protecting privacy. Digital identity can be through a government, such as eID in Estonia and Lithuania, or a financial institution, such as BankID in Sweden and Norway.[38]

---

34 'Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing' (3 December 2018), issued by the US Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, FinCEN, the National Credit Union Administration and the Office of the Comptroller of the Currency.

35 World Bank Group, 'Private Sector Economic Impacts from Identification Systems'.

36 Capgemini, World Payments Report 2020.

37 McKinsey & Company, The 2020 McKinsey Global Payments Report.

38 European Union Agency for Cybersecurity (ENISA), 'eIDAS compliant eID Solutions'.

Verification systems for digital identification present several risks, as noted in FATF's Digital Identity guide.[39] Among the risks are identity theft, forged or tampered source documents, misuse of data owing to unauthorised access and the potential for data theft when communicating via the Internet. It is estimated that synthetic identity fraud, where criminals use fake identification to secure credit, is the fastest-growing type of financial crime in the United States and costs lenders worldwide an estimated US$6 billion.[40]

Regulators have implemented rules for reliance on digital identity verification. The 5AMLD states that an obliged entity must identify the customer, which can be based on traditional documentary evidence or information obtained from a reliable and independent source, including electronic identification means.[41] Those electronic identification methods must comply with Regulation (EU) No. 910/2014, which sets out criteria for identity verification services.

The United Kingdom's Joint Money Laundering Steering Group indicates that digital identification may provide satisfactory evidence of identity on its own, but it must use data from multiple sources across time, incorporate qualitative checks that assess the strength of the information supplied or be performed through an organisation that meets the relevant EU criteria.[42]

Recent typology trends

As AML legislation has become more stringent and financial institutions have correspondingly strengthened their processes, criminals' preferred methods have shifted. While there are numerous money laundering typologies, this section focuses on four that have received more attention from regulators and appear to be increasing in prominence.

Trade-based money laundering

Trade-based money laundering (TBML) is the process of disguising proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise illicit origins.[43] Of the three broad methods of money laundering (using financial

39 FATF, 'Digital Identity'.

40 Bryan Richardson and Derek Waldron, 'Fighting back against synthetic identity fraud', McKinsey & Company (2 January 2019).

41 Directive (EU) 2018/843.

42 Joint Money Laundering Steering Group, 'Prevention of money laundering/combating terrorist financing (2020 revised version)'.

43 FATF, 'Trade-Based Money Laundering' (June 2006), page 5.

institutions, physically smuggling cash and using the international trade system), the FATF has found that the abuse of the international trade system has historically received relatively little attention.[44] TBML is notoriously difficult to detect because it is integrated into the economy through a trade transaction.

To counter the risk of enabling TBML, companies should assess their risk and consider the relevant red flags. Financial institutions should factor TBML in their risk assessment and implement sufficient controls for reviewing trade documentation supporting letters of credit and how they monitor the payment messages for open trade transactions.[45]

In December 2020, the FATF issued updated guidance regarding TBML,[46] noting that the exploitation of TBML techniques is particularly effective when there is a complicit relationship between the importer and exporter, who are actively misrepresenting the trade or invoice process. It further points out that authorities can have a greater impact if they disrupt these complicit actors through criminal prosecution or removing their authority to trade.

Ransomware

The use of ransomware is increasing in popularity and can be a method to launder money. According to a recent CyberEdge Group survey, 62 per cent of organisations were victimised by ransomware in 2020, up from 56 per cent in 2018 and 55 per cent in 2017. It points out the increase may be fuelled by the dramatic increase in ransomware payments – 58 per cent paid the ransom in 2020, compared with 45 per cent in 2018 and 39 per cent in 2017.[47]

One of the 22 AML predicate offences that was harmonised across the EU within Directive (EU) 2018/1673 is cybercrime, which includes ransomware. In October 2020, the European Union Agency for Cybersecurity issued a threat landscape guidance document regarding ransomware.[48] The document indicated that €10.1 billion was paid in ransom during 2019, more than €3.3 billion more than in 2018, and that 45 per cent of attacked organisations paid the ransom.

---

44 ibid.

45 The Wolfsberg Group, 'The Wolfsberg Group, ICC and BAFT Trade Finance Principles (2019 amendment)' (27 March 2019).

46 FATF and the Egmont Group, 'Trade-Based Money Laundering: Trends and Developments' (December 2020).

47 Cyber Edge Group, 'Cyberthreat Defense Report 2021'.

48 ENISA, 'ENISA Threat Landscape 2020 – Ransomware'.

In November 2021, FinCEN issued an advisory for financial institutions regarding the increase in ransomware and the associated financial red flag indicators.[49] The advisory points out that ransom is most often paid via virtual currencies. The victim pays the perpetrator via their bank account to a virtual currency exchange. The perpetrator then transfers the virtual currency, typically bitcoin, through several transfers using mixers and tumblers[50] to obscure the money trail or through trasnfer of the virtual currency to an exchange in a jurisdiction with weak AML controls.

Human trafficking and modern slavery

Human trafficking is one of the most profitable criminal enterprises, generating an estimated US$150 billion per annum.[51] Human trafficking from Africa and Asia into Europe is relatively well known, particularly where refugees from war-ravaged countries, including Syria, Iraq and Afghanistan are exploited by traffickers for large sums and subjected to dangerous conditions. Modern slavery, or forced labour, still occurs today, even in Europe, and is becoming more prominent.

FinCEN recently issued an updated advisory regarding human trafficking.[52] It points out that effects of the covid-19 pandemic (eg, travel limitations, shelter-in-place orders and teleworking) may exacerbate the conditions that contribute to human trafficking and affect the existing red flag indicators.

Since the previous advisory in 2014, it identified an additional 10 financial and behavioural indicators of labour and sex trafficking, bringing the total to 20. It notes that human traffickers and facilitators have used front companies, exploitative employment practices, funnel accounts and alternative payment methods to facilitate money laundering. Some of the newly added red flags include frequent transactions with online classified sites based in foreign jurisdictions and the frequent sending or receipt of funds via cryptocurrency to or from darknet markets associated with illicit activity.

---

49 FinCEN advisory, 'Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments', FIN-2021-A004 (8 November 2021).

50 Services offered to mix potentially identifiable cryptocurrency funds with others to obscure the origin.

51 Estimate from the International Labour Organization.

52 FinCEN advisory, 'Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity', FIN-2020-A008 (15 October 2020).

Human trafficking and modern slavery fall under environmental, social and governance (ESG) considerations, criteria to which stakeholders, including investors, business partners, employees and consumers, are increasingly looking to assess the holistic performance of a company. Regulators are applying a corresponding increase in scrutiny of these areas, and it is likely that enforcement will also increase.

Illegal wildlife trade

Illegal wildlife trade is a major transnational organised crime, generating criminal proceeds estimated at between US$7 and US$23 billion each year.[53] Wildlife crime has been linked to drug, human and arms trafficking. Similar to human trafficking and modern slavery, the illegal wildlife trade is an important component of ESG considerations and is again likely to see increased attention from both stakeholders and regulators.

A FATF report from June 2020 noted that countries rarely investigate this crime and that neither governments nor the private sector have prioritised efforts to combat this risk.[54] The report states that criminals misuse the legitimate wildlife trade and other import/export businesses as a front to hide illegal proceeds from wildlife crimes. They also note an increase in the role of online marketplaces and mobile and social media-based payments to facilitate movement of proceeds from wildlife crimes.

In the EU, environmental crime, including the illegal wildlife trade, is captured by Directive 2018/1673 as a predicate offence to money laundering. This means that obliged entities should consider illegal wildlife trade in their risk assessment.

The push towards AML effectiveness

There has been a growing drumbeat over the past couple of years for evaluating whether global AML efforts have led to an appreciable reduction in predicate crimes and increased asset forfeiture or merely an increase in the cost of compliance. There has been renewed focus on specific actions that may lead to greater AML effectiveness, such as including risk-based procedures by both regulators and obliged entities, the ability to link an obliged entity's risk assessment to national AML priorities, continuing to increase information sharing and leveraging technology.

53 According to a 2016 UN report.

54 FATF, 'Money Laundering and the Illegal Wildlife Trade' (June 2020).

FATF strategic review

This conversation regarding effectiveness versus mere implementation of rules picked up steam when the FATF announced in late 2019 that it was planning a strategic review of its evaluation process. At the time, the executive secretary of the FATF stated that its evaluation of effectiveness focused more on process than outcome.

The executive secretary further stated that the evaluation process is very effective in motivating countries to take action, but the motivation is generally to avoid a bad report rather than reducing harm to society or protecting the integrity of the financial system. He said that the fourth round of FATF evaluations – the first to focus on effectiveness – showed that countries were taking a tick-box approach to regulatory compliance and focusing on processes rather than outcomes.[55]

In the June 2020 FATF Plenary, delegates agreed that the aim of future evaluations would be to make them more timely, have a greater emphasis on effectiveness and strengthen the risk-based elements of the assessment process.[56]

What regulators can do differently

Transitioning from rule-based supervision to risk-based supervision takes time and can be challenging, as the FATF February 2021 Plenary summary stated. It requires a change in supervisory culture where supervisors have an in-depth understanding of the risks that their regulated entities face.[57] The FATF consequently issued risk-based supervisory guidance in March 2021, which focuses on supervisors' understanding of risk and applying their strategy based on those risks.[58]

There are two key ways in which regulators can take action to support greater effectiveness in countering money laundering. The first is to help financial institutions and other obliged entities by providing guidance on linking the national risk assessment to the entity's risk assessment.

Detailed risk guidance, along with the entity's knowledge of its business, is useful to financial institutions and other obliged entities in helping to determine where their risk of money laundering is greatest and how they might mitigate those risks. The

55 FATF, 'Remarks at the RUSI meeting on the Financial Action Task Force Strategic Review' (18 November 2019).

56 FATF, 'Outcomes FATF Virtual Plenary, 24 June 2020'.

57 FATF, 'Outcomes FATF Plenary, 22, 24 and 25 February 2021'.

58 FATF, 'Guidance for a Risk-Based Approach: Supervisors' (March 2021).

4AMLD mandated that the European Commission conduct an assessment of money laundering and terrorist financing risks affecting the internal market and update it at least every two years.

The most recent EU-wide risk assessment focuses on vulnerabilities at the EU level, both in terms of legal framework and effective application, and provides recommendations for addressing the identified risks.[59] The description of money laundering risks within the European Union is relatively detailed. For example, within the gambling sector, it points out that land-based betting is high risk owing to typically ineffective controls, whereas online gambling is high risk owing to very large numbers of transactions and the lack of face-to-face interaction.

The 5AMLD mandated that member states make the results of their risk assessments available to the European Commission and the other member states, and make a summary version, without classified information, publicly available.

Another way in which regulators can support effectiveness in AML efforts is providing specific feedback regarding STRs. The headlines surrounding the 'FinCEN Files' garnered a great deal of attention regarding the volume of STRs that did not appear to result in any action taken.

In fairness, it is unclear how individual STRs are collated with other information and considered by the respective FIU; however, most observers see an excessive amount of low-quality STRs being filed from a defensive position. The penalty for not filing an STR may be great, but there is no penalty for submitting an STR that may not prove warranted or has little probative value.

What financial institutions can do differently

Some areas of improvement that would make financial institutions more effective in combatting money laundering are not within their control, particularly the creation of complete and accurate UBO registers; however, there are two areas where financial institutions can take action: creating and maintaining risk assessments with proper governance and oversight, and sharing information.

59 COM(2019) 370 final, Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (24 Jul 2019).

The EBA recently issued revised guidance regarding risk factors for money laundering and terrorist financing.[60] The guidelines note that risk assessments should be performed at least annually or more frequently when necessary, and that they should always consider specific sources of information, including the European Commission's supranational risk assessment referenced above.

The second action financial institutions and other obliged entities can take in support of greater AML effectiveness is to participate in information sharing. Money launderers often move funds between jurisdictions to make it more difficult to investigate and trace the source of funds.

Examples of public–private partnerships

United Kingdom

The Joint Money Laundering Intelligence Taskforce (JMLIT) is a partnership between law enforcement and financial institutions. They exchange information related to financial crime, including money laundering.

Since its inception in 2015, JMLIT has supported numerous law enforcement investigations, while the participating financial institutions have identified over 5,000 accounts suspected of money laundering, began 3,500 of their own internal investigations and used the information obtained to enhance their systems of controls and monitoring.

In addition to suspicious accounts, they can also share information related to emerging typologies that may allow financial institutions to identify potentially suspicious behaviour at an earlier stage.

Netherlands

At the encouragement of the Dutch regulator, in 2019 four Dutch banks (ABN AMRO, ING, Rabobank and Volksbank) signed a covenant with the National Police and the FIU to help identify people who facilitate crime. The authorities believe a small group of enablers, financial advisers, tax advisers, notaries, accountants and lawyers play a key role in laundering drug money in the Netherlands. The law enforcement agencies will provide information to the banks, which will compare it with their KYC and transaction data.

60 EBA/GL/2021/02, Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849 (1 March 2021).

Examples of private–private partnerships

Estonian banks

In the wake of the money laundering scandals that recently occurred in Tallinn, Swedbank, SEB, Luminor, LHV, Bigbank, Citadele, OP Bank, Coop, TBB and Inbank all partnered with the Estonian tech company Salv to create an information and data exchange platform. The platform, known as AML Bridge, has thus far prevented up to €3million from reaching criminal-controlled accounts after more than 1,200 'collaborative investigations have been undertaken legally, securely, and efficiently across three different use cases – AML, fraud, and sanctions'.[1]

Dutch banks

The three largest banks in the Netherlands (ABN AMRO, ING and Rabobank) began a pilot programme to share KYC information, such as data on beneficial owners and organisational charts, where those clients have consented. They are trying to determine whether this information sharing can reduce costs and give compliance departments access to better, more timely KYC data.

Nordic banks

The five largest lenders in the Nordics (Danske Bank, DNB, Handelsbanken, Nordea and SEB) disclosed plans to share KYC data on large and medium-sized corporates with the goal of streamlining due diligence, similar to the initiative by the Dutch major banks.

TMNL

The Transaction Monitoring Netherlands (TMNL) partnership between five Dutch (ABN AMRO, ING, Rabobank, Triodos Bank and Volksbank) is operational and will begin joint monitoring of business payment transactions.[2]

---

1 Karl Flinders, 'Estonian anti-money laundering software pilot reaps benefits', *Computer Weekly* (16 March 2022).

2 Transaction Monitoring Netherlands website (https://tmnl.nl/).

There has been guidance encouraging the sharing of information related to money laundering for quite some time to address this issue. The FATF has made several recommendations, as have some national regulators. There is now an increasing trend

of public–private partnerships and, in some cases, financial institutions sharing information directly with each other.

Legislation protecting the privacy of personal data poses challenges to information sharing; however, some regulators are providing assurances regarding information sharing in the AML context.

In December 2020, FinCEN published updated guidance,[61] which gave great latitude in financial institutions' ability to share relevant information with each other. The guidance specified that the financial institution does not need to have specific information regarding proceeds of a crime or have made a conclusive determination that the related activity is suspicious. It also stated that information on attempted transactions and information that includes personally identifiable information can be shared, and financial institutions are not restricted in their methods of sharing information, including verbally.

Key elements in an AML programme

A study from 2005 showed that in addition to the penalty a financial institution incurs for an AML failure, it also loses share value and business opportunities owing to reputational damage. Furthermore, remediation costs over the first 18 months are typically 12 times greater than the fine itself.[62]

Proactively addressing weaknesses in an AML compliance programme is a smart long-term proposition. The US Federal Financial Institutions Examination Council (FFIEC) publishes a comprehensive inspection manual that outlines the key elements of a BSA/AML programme.[63] The following table identifies key elements from the FFIEC manual and our suggested questions to guide your organisation's planning.

61 FinCEN, Section 314(b) Fact Sheet.

62 Joshua Fruth, 'Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states', *Reuters* (14 March 2018).

63 Federal Financial Institutions Examination Council, BSA/AML Examination Manual (2014).

US FFIEC's key elements to a BSA/AML programme	Key questions for your organisation to consider
Risk assessment	
The risk assessment should identify the specific risk categories applicable to the institution (eg, products, services, customers and geographies) and contain a more detailed description of the specific risks within those categories that are applicable to the institution.	• Is there a documented risk assessment? • Does the risk assessment include all relevant risks? • Does the risk assessment consider relevant national or supranational risk assessments? • Is there proper governance and oversight of the risk assessment process? • How often and under which circumstances is the risk assessment updated? • Has the risk assessment considered changes owing to global events (eg, pandemics and wars), specifically differences in staffing and STR?
AML compliance programme	
The AML compliance programme should be documented and approved by the board of directors.	• Is the AML programme properly documented with sufficiently detailed policies and procedures? • Are controls in place to ensure compliance with policies and procedures outlined in the AML programme? • Do the policies, procedures and controls outlined in the AML programme sufficiently correspond to and mitigate the risks outlined in the risk assessment? • Do the controls outlined identify higher-risk operations, provide reporting methods to the board of directors, identify personnel responsible for AML compliance, address record-keeping requirements, implement risk-based customer due diligence (CDD) policies, contain detailed procedures for STR, address segregation of duties and address the process for anomalous transaction reporting? • Are AML responsibilities included within job descriptions? • Is there an incentive component for first-line employees to act in compliance with the AML programme?
Independent testing	
The controls outlined in the AML compliance programme should be subject to independent testing by a suitably experienced person whether from internal audit, external audit, consultants or other qualified parties.	• Is there independent testing of the AML programme (including risk assessment and controls)? • Is the testing performed in a risk-based fashion? • Does the testing include evaluation of the risk assessment, policies and procedures, deficiency remediation, training, suspicious activity monitoring and the relevant information systems used within the AML programme? • How often does independent testing occur? • Are the results of the testing communicated to the board of directors? • Do the results of the testing inform future revisions of the AML risk assessment?

US FFIEC's key elements to a BSA/AML programme	Key questions for your organisation to consider
Training	
All relevant personnel should be trained in both regulatory requirements and the entity's AML policies and procedures. The training should be specific to the organisation; for example, a bank's training may focus on transaction monitoring whereas a shipping company may focus on how to identify red flags in trade-based money laundering.	• Does the training cover all relevant personnel? • Does the training incorporate lessons learned from their industry or institution? • Is the training tailored to the person's specific responsibilities? • Do those charged with overseeing the AML programme receive regular training regarding regulatory requirements? • Is the board of directors and executive management informed of their AML regulatory requirements?

Conclusion

AML risk management has become more challenging over time as regulations have become more stringent, and financial institutions, in particular, have faced larger fines where compliance programmes have been deficient.

However, it is also a time in which more detailed guidance is being developed by government[64] and non-government[65] bodies to help build robust AML programmes, technology is being developed to help entities become increasingly sophisticated in their ability to detect and monitor suspicious transactions, and partnerships are being developed to share information that allows for a more comprehensive compliance effort.

When evaluating compliance efforts, entities should be proactive, develop a robust AML compliance programme and pay particular attention to the CDD, UBO and transaction monitoring elements of that programme. As part of this effort, entities should:

- keep up to date on changing legislation and regulations;
- consider new and evolving technologies and typologies in the overall risk assessment;
- where possible, share information when it allows for a more comprehensive solution to identifying money laundering; and
- understand where to focus efforts to work towards greater AML effectiveness.

64 FCA, 'Financial Crime Guide: A firm's guide to countering financial crime risks (FCG)' (February 2022).

65 Basel Committee on Banking Supervision, 'Sound management of risks related to money laundering and financing of terrorism: revisions to supervisory cooperation' (2 July 2020).

CHARLIE STEELE
Forensic Risk Alliance

Charlie Steele is a partner in FRA's Washington, DC office with more than 30 years of government and private-sector experience in civil and criminal compliance, investigations, enforcement and litigation matters in a variety of industries and sectors. In recent years, he has specialised in economic sanctions and Bank Secrecy Act and anti-money laundering (BSA/AML) matters.

He is a former senior US Treasury Department and Department of Justice official, serving most recently as Chief Counsel for the Office of Foreign Assets Control (OFAC). In that role, he led the team of lawyers providing legal advice and support to OFAC and other Treasury Department personnel in the formulation, implementation and enforcement of economic sanctions.

Charlie has also served in a number of other senior positions in the Treasury Department: associate director for enforcement in OFAC, deputy director of the Financial Crimes Enforcement Network (FinCEN, the US government's principal BSA/AML agency and the US financial intelligence unit) and deputy chief counsel in the Office of the Comptroller of the Currency (the US supervisor and regulator of national banks).

BHAVIN SHAH
Forensic Risk Alliance

Bhavin is a partner in FRA's Dubai office. He has more than 18 years' experience in professional services, focusing on financial institutions, sovereign wealth funds, investment companies, development institutions and regulators. Based in the region since 2009, Bhavin has served clients across Asia, the Middle East, Africa, America and Europe.

Bhavin's expertise lies in complex legal matters, and forensic and crisis management across the Middle East and North Africa region. He has advised on high-profile cases for clients such as Unicorn Bank, Arcapita, Standard Chartered, Riyad Bank and SABB. He has also advised central banks and capital market authorities across the region and globally on special situations and monitorships.

Bhavin is a trusted adviser to boards of directors, CXOs, governments and regulators. His experience with authorities includes advising ministries, central banks and other government bodies on various strategic initiatives. He is commended by clients for his ability to go into a crisis and transaction environment and drive change through both strategic and surgical measures. He has also taken interim management roles to help efficiently navigate through turnaround plans and communicate with stakeholders.

Previously, Bhavin led the financial services proposition within the financial advisory practice for Deloitte in the Middle East. He was also directly responsible for conceptualising, building and leading the financial services regulatory advisory practice, which provided a wide range of specialised services to clients on topics related to complex regulatory matters, including financial crime, sanctions and consumer protection.

GERBEN SCHREURS
Forensic Risk Alliance

Gerben Schreurs is a partner in FRA's Zurich office and has over 25 years of experience solving technical challenges on complex problems requiring insight into large (un)structured data sets, including matters relating to investigations, risk management and compliance. He leads high-profile and confidential cases in the areas of fraud, information leakage, money laundering, disputes and regulatory breaches.

Gerben has supported many clients across the globe with the creation of analytics solutions aimed at preventing fraud loss or reputational damage. One key innovation he led in the area of transaction surveillance involved developing a bespoke analytical solution that combined multiple factors to identify potential risk behaviour in transactional patterns. This project, which was a departure from industry standard, brought together compliance, legal, data science and technology professionals to shape the approach.

Prior to joining FRA, Gerben served as the global head of systems and controls for financial crime compliance at Credit Suisse. Gerben managed a team of over 50 people internationally and was responsible for the operations and uplifts to compliance systems, with the aim of making processes more efficient and reducing regulatory risks by applying a consistent approach globally.

Gerben previously served more than 20 years in KPMG, where he was the global lead partner responsible for the forensic technology team, focusing on topics relating to data analytics, cybersecurity and e-discovery.

SARAH WRIGLEY
Forensic Risk Alliance

Sarah Wrigley is a director based in FRA's London office. She has over 18 years' experience in complex, cross-jurisdictional investigations, including financial crime and sanctions, regulatory issues and accounting irregularities. She has worked across a range of industries, with a focus on financial services.

Prior to joining FRA, Sarah was the Africa and Middle East regional head of financial crime intelligence and investigations for Standard Chartered Bank. Sarah led the bank's investigation response in the region to global financial crime issues generating media and regulatory scrutiny. She led a team developing proactive intelligence on emerging financial crime themes covering money laundering and predicate offences, terrorist financing and potential sanctions breaches in order to identify and investigate higher risk clients.

Sarah previously spent 11 years in the forensic accounting team of a Big Four firm and has led investigations into corporate and procurement fraud, embezzlement, regulatory breaches, accounting misstatements and bribery and corruption. Sarah is a UK-qualified chartered accountant, a certified fraud examiner and a certified anti-money laundering specialist.

DEBORAH LUSKIN
Forensic Risk Alliance

Deborah Luskin is an associate director in FRA's Washington, DC office with over 13 years experience in auditing and consulting. Deborah has experience in forensic accounting, financial audit attestation, risk management assessments, Sarbanes-Oxley 404 readiness and audit attestation and service organisation internal control assessments.

Deborah is currently providing forensic accounting support for a financial institution's anti-money laundering review. She previously worked with a global manufacturing firm accused of bribery in connection with a Middle Eastern entity, provided support for a corporate monitorship of a Tier 1 financial institution and worked with a global manufacturing company and their external counsel in response to an investigation by the Serious Fraud Office and the Parquet National Financier into bribery and corruption.

Prior to joining FRA, Deborah spent nine years at a Big Four company working in risk management. Deborah specialised in assessing both financial and information systems internal controls, supporting the financial statements, assessing regulatory compliance, performing fraud evaluations and assessing risk management programme effectiveness. Deborah led large multinational teams in various industries.

Deborah is a certified public accountant, a certified anti-money laundering specialist, a certified fraud examiner, a certified in financial forensics, a certified information systems auditor and a certified information systems security professional.

Forensic Risk Alliance (FRA) is a forensic accounting, data governance and compliance consultancy firm specialising in international corruption and fraud investigations for major global corporations and law firms. For more than 20 years, FRA has offered extensive multi-jurisdictional data privacy, transfer, and protection expertise to help clients achieve their objectives with compliance, litigation and investigations. With over 200 employees, FRA is headquartered in London – one of 11 locations across Europe, the Middle East and Africa and North America. FRA has extensive cross-sector and cross-border experience and scalability anywhere in the world, with globally integrated teams across both developed economies and emerging markets, having worked in more than 75 countries and with the capability to speak over 30 languages.

Audrey House
16-20 Ely Place
London EC1N 6SN
United Kingdom
Tel: +44 20 7831 9110
www.forensicrisk.com

Charlie Steele
csteele@forensicrisk.com

Bhavin Shah
bshah@forensicrisk.com

Gerben Schreurs
gschreurs@forensicrisk.com

Sarah Wrigley
swrigley@forensicrisk.com

Deborah Luskin
dluskin@forensicrisk.com

Compliance in France in 2022

Ludovic Malgrain, Jean-Pierre Picca and Grégoire Durand*
White & Case LLP

IN SUMMARY

The year 2021 and early 2022 proved eventful for compliance and white-collar crime in France, especially for anti-bribery and compliance activity. Agencies are continuing to build on Sapin II by incrementally defining anti-corruption standards and stepping up their enforcement efforts on both the administrative and judicial fronts.

DISCUSSION POINTS

- Sapin II and its lasting impact on French anti-bribery law
- Aggressive white-collar crime strategy and the success of CJIPs in enforcement actions
- Court of Cassation cases on successor liability and criminal corporate liability
- Reform of the blocking statute
- Duty of Vigilance Law and proposed EU directive on sustainability due diligence

REFERENCED IN THIS ARTICLE

- Sapin II
- OECD corruption working group's report on France's anti-bribery efforts
- 2021 revised AFA Anti-Corruption Guidelines
- Case No. 18-86.955, 25 November 2020 on successor criminal liability
- 2021 revised AFA Guidelines
- AFA guidance on gifts and invitations policies, construction and internal investigations
- 2021 revised AFA guidance on anti-bribery verifications in M&A
- 2020 CNIL guidance on personal data in whistle-blowing procedures
- CJIP agreements of 29 January 2020 and 26 February 2021
- 2021 CRPC cases for physical persons in conjunction with CJIPs
- 2017 Duty of Vigilance Law
- 2022 EU proposal for a directive on corporate sustainability due diligence

The year 2021 was again a year of consolidation for France's compliance, investigations and white-collar crime ecosystem, with limited statutory changes (2022 being an electoral year in France) and a few noteworthy developments from courts and administrative agencies. After making great strides since the country heightened its anti-corruption standards with the Law of 9 December 2016 on transparency, corruption and modernisation of the economy (Sapin II), France and its authorities have since demonstrated that they are now key players in the global white-collar crime and anti-bribery landscape.

In anti-bribery compliance in particular, the French Anti-Corruption Agency (AFA) keeps building on Sapin II by providing guidance on specific topics, auditing compliance programmes of private and government entities and bringing cases in front of its sanctions board (although no new cases were heard in 2021 and early 2022).

The judicial part of this effort also proved newsworthy in 2022, with the National Financial Prosecutor's Office (PNF) continuing to seek high fines against corporate defendants as part of judicial public interest agreements (CJIP),[1] and other regional prosecutors stepping in to do the same. A decision from the Paris Court of Appeal in a case against a major foreign bank also showed, by significantly reducing the amount of what had been the highest fine ever imposed in the French system, that courts remain a valid option for corporate defendants despite the increased use of transactional tools.

Bribery and corruption issues still occupied the centre stage of the compliance and white-collar crime landscape, but some other areas of compliance law have recently seen renewed interest. Environmental, social and governance (ESG) issues have been a staple of French compliance law since the 2017 Duty of Vigilance Law mandated large corporations to create and publish a dedicated vigilance plan and exposed non-compliant corporations to a potentially large liability risk.

While to date very few cases tested the actual implementation of the Duty of Vigilance Law (recent decisions being largely procedural), the risks associated with those issues may resurface as in early 2022 the EU commission proposed a draft directive[2] that would extend some aspects of the French and German duty of vigilance regimes to the European Union.

1 The French equivalent of deferred prosecution agreements.

2 Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937.

Overall – and considering the continuing disruptions resulting from the covid-19 pandemic that have slowed down the French economy and its legislative and judicial systems – the French compliance landscape is expected to continue evolving incrementally this year, at least until the end of the electoral period in June 2022. Noteworthy changes on specific issues, however, could come from courts and administrative agencies such as the AFA.

Building on the paradigmatic change of Sapin II since 2016

When assessing the French anti-bribery landscape in its late 2021 assessment report,[3] the Organisation for Economic Co-operation and Development's working group on bribery noted that since its last assessment in 2014, France has carried out 'a significant number of reforms' that have provided France with 'a modern institutional framework and legal tools to combat foreign bribery more effectively'.

Among those key reforms was Sapin II, which is France's comprehensive anti-corruption reform and a response to laws such as the US Foreign Corrupt Practices Act and the UK Bribery Act. The law toughened sanctions on corruption, imposed stringent compliance obligations on large corporations and created the AFA.

As a reminder, since June 2017, companies incorporated in France and exceeding a certain size threshold[4] are required to have an anti-corruption compliance programme. Presidents, directors and managers of qualifying companies may be held personally liable for failure to implement such a compliance programme.

Compliance programmes under Sapin II that are tailored to prevent acts of bribery and influence peddling must include the following measures aimed at preventing corruption:

- a code of conduct;
- an internal whistle-blowing mechanism;
- regularly updated corruption risk mapping;
- a risk assessment (risk mapping) process;
- third-party due diligence procedures;

---

3 Organisation for Economic Co-operation and Development working group on bribery, Implementing the OECD Anti-Bribery Convention in France: Phase 4 Report (December 2021).

4 This requirement, according to article 17 of Law of 9 December 2016 on transparency, corruption and modernisation of the economy (Sapin II), applies to any private company or public entity of an industrial or commercial nature that has (1) more than 500 employees or is part of a corporate group whose parent company is headquartered in France and employs more than 500 people; and (2) whose annual turnover or annual consolidated turnover exceeds €100 million.

- accounting controls;
- training programmes for employees exposed to high risks of corruption and influence peddling;
- a disciplinary procedure; and
- an audit mechanism to assess the effectiveness of the compliance programme.

Based on the AFA audits and sanctions procedures of private entities conducted to date, the agency pays extremely close attention to the risk-mapping process (which is supposed to inform all other measures), the code of conduct and the top management's commitment to anti-bribery. Corporations that are subject to the above-mentioned requirements should be aware that merely having the required measures in place is not sufficient as the AFA controls their quality and practical implementation.

Sapin II also introduced major procedural changes for white-collar cases, with the creation of the equivalent of the deferred prosecution agreement (DPA): the CJIP.[5] It gives prosecutors a transactional tool to negotiate with corporate plaintiffs for a limited number of offences, including:

- active public agent bribery and influence peddling offences (eg, active foreign public agent bribery);
- active and passive private bribery offences (private 'commercial' bribery or sports bribery);
- tax fraud (since 2018);
- laundering proceeds of tax fraud;
- substantial harm to the environment (since 2020).

Once frowned upon by the French legal community, which is traditionally reticent on transactions in criminal law, the CJIP is now a popular tool. While some of its limits are now being tested, in particular regarding the treatment of physical persons, it has proved essential to the resolution of many high-profile cases, particularly those involving international cooperation, and has allowed France to levy more than €3 billion in fines since 2017.

5 Article 41-1-2 of the Criminal Procedure Code. For more information on audits of the French Anti-Corruption Agency (AFA), see also AFA's 'Investigation Charter' (last updated in April 2019) on the rights and duties of AFA auditors and audited entities.

Sapin II anti-bribery compliance requirements

Throughout 2021 and early 2022, the AFA continued its audits at corporations that are mandated by article 17 of Sapin II to have anti-corruption compliance programmes. Carried out at the initiative of the AFA's director or upon the request of authorities (or approved non-governmental organisation (NGOs)), the audits verify that the company has proper compliance programmes in place.

Although AFA investigators do not have the police powers required for coercive searches (unlike competition, tax or judicial police dawn raids), they can request any information or professional document that is useful for the audit and can conduct interviews with managers and employees. Audited corporations cannot claim professional secrecy to decline to answer questions or requests for documents, and individuals or entities may be fined in the case of obstruction.[6]

In addition, pursuant to article 40 of the Criminal Procedure Code, the AFA must report any wrongdoing it discovers as part of its mission. This means – the agency's audit questionnaires being extremely broad – that it frequently refers wrongdoing it discovers to prosecutors (either the PNF or local prosecutors).

The agency referred three cases in 2020 (and, in total, 14 cases since its creation in 2017).[7] The AFA regularly receives reports from third parties, which may inform its decision to audit an entity (for 17 per cent of audited entities, a credible report was received), and several reports received by the agency in 2020 were directly forwarded to a prosecutor's office.

In 2020, the AFA initiated 19 new audits of private entities, ranging from €1.4 billion to €200 billion in turnover, and from 2,700 to 179,000 employees.[8] To date, it has carried out 125 audits of public and private entities since its creation in 2017.

In 2022, and now that the substantial reduction of its scope considered earlier in 2022 was dropped by legislators, the AFA is expected to continue carrying on its mission across industries.

In 2019 and 2020, the first two cases were brought by the AFA's director to its independent sanctions board for allegedly defective anti-bribery compliance programmes. Additional hearings on these cases were held in 2021, but no other new case was brought to the sanctions board.

---

6 Article 4 of Sapin II. No case of obstruction was reported in 2020.

7 AFA, 2020 Annual Report, page 19.

8 id, page 17.

The agency's first case, brought on charges of defective risk mapping, code of conduct and third-party evaluation procedure, was dismissed by the sanctions board, noting for some charges that the corporation had taken swift and appropriate remedial actions after the AFA inspection pointed out some flaws in its programme. The decision also confirmed the non-binding status of the AFA's recommendations.

The second case concerned multiple counts of non-compliance with Sapin II and led the sanctions board, for the first time, to enjoin the company to adapt its code of conduct (which did not contain the elements mandated by law and merely redirected to another policy) and accounting controls under penalty of a fine. In July[9] and November 2021,[10] the sanctions board decided that the company had now complied with these two injunctions, thus ending the proceedings.

While no sanction per se has been imposed to date, the cases helped establish the AFA as a key enforcement player in the French compliance space and as a credible threat to entities that are being investigated and audited.

The AFA has also integrated some elements of the cases in its new recommendations, notably restating that they have no legal force but that an entity stating that it has followed those guidelines benefits from a prima facie presumption of compliance with the law. In turn, similar to the 'comply or explain' principle used in corporate governance, an entity subject to article 17 of Sapin II that decides not to follow some of or all the recommendations must demonstrate that its choices enable it to meet the requirements of Sapin II.

Revision of AFA's main anti-corruption guidelines

On 12 January 2021, the AFA officially published its new guidelines on anti-corruption programmes (the Recommendations).[11] In its revised 2021 version, the AFA built on its 2017 guidance by adding practical considerations gathered from its advisory and audit missions, industry feedback and, in certain cases, the first AFA sanctions board cases in which non-compliance with the Recommendations was a key issue. They include the following elements, among other things:

- for the first time, a set of high-level recommendations applicable to all entities regardless of their public or private status or their obligation to enact a compliance programme under article 17 of Sapin II;

9 AFA Sanctions Board Decision No. 19-2 of 7 July 2021, *Société I SA*.

10 AFA Sanctions Board Decision No. 19-2 of 30 Nov. 2021, *Société I SA*.

11 AFA, The French Anti-Corruption Agency Guidelines (12 January 2021).

- an increased focus on the top management's involvement, which the Recommendations define more precisely, as they are personally accountable for the entity's compliance with its obligations under article 17 of Sapin II; and
- a confirmation of the importance of risk mapping, which should constitute the first step of the compliance programme and must permeate the other measures (code of conduct, training, etc) based on the corruption risks it identified.

In July 2021, the AFA released a new version of the questionnaire used to audit companies.

Corporate guidance updates and industry-specific guidelines

Another illustration of the AFA's proactive approach is its effort to provide guidance on gifts and invitations, conflicts of interest and internal investigations. Until recently, there was no official guidance on some of those topics for the private sector in France, and large multinational corporations often modelled their policies on standards applicable in other countries or used a single global policy without any local adaptation. This 'copy and paste' approach sometimes failed to account for local specificities, such as the explicit prohibition by the Criminal Code of private-to-private bribery.

Theses guides are intended to help entities draft their anti-corruption policies. They are not legally binding, but synthetically restate applicable law and will serve as a useful reference tool to draft a policy that takes into account the specificities of French law, regardless of whether the entity can be audited by the AFA.

In September 2020, the AFA published a definitive version of its guide on gifts and invitations policies for corporations, associations and foundations,[12] offering step-by-step guidance on the items to consider when drafting a policy (whether to set fixed maximum amounts, transparency and accounting considerations, etc), as well as examples of problematic conduct that a good policy should prevent.

In November 2021, the AFA also released its guide to preventing conflicts of interest in the workplace to help identify risky situations and define mitigation measures. The AFA includes examples of best practices it encountered in the course of its audit and advisory missions.

12 AFA, Practical Guide: Gifts and hospitality policy in private and public sector corporations and non-profits (11 September 2020).

Finally, in December 2021, the AFA published its final practice guide on anti-corruption for small and medium-sized enterprises and small businesses. These companies cannot be audited by the AFA, but the AFA insists that there is a real advantage in those companies taking steps to prevent corruption as it enables them not only to prevent acts of corruption and their financial, reputational and human consequences, but also to demonstrate their integrity to their business partners.

This guide will be of particular interest to multinational corporations with a small to medium-sized presence in France (ie, that do not cross the legal threshold to be audited by the AFA) as this provides a useful all-in-one compendium of baseline French anti-corruption rules and practices.

Below are examples of guides released by the AFA in 2021 and 2022:

- a guide on anti-corruption due diligence for mergers and acquisition;
- a draft of a guide on anti-corruption accounting controls in companies;
- a guide dedicated to the construction sector (which is the AFA's first sector-specific guide and will serve, in particular, the agency and the government's goal to promote integrity in major sports events, such as the Paris 2024 Olympic Games[13]); and
- a draft of a guide to internal anti-corruption investigations.

New avenues for enforcement

The December 2020 Law on the European Public Prosecutor's Office and Specialised Justice[14] created a specific CJIP procedure to deal with cases of substantial harm to the environment, chargeable under the criminal provisions of the Environmental Code, with a specific monitoring procedure by specialised environmental agencies after a deal has been reached and judicially approved.

The first environmental CJIP[15] was approved on 16 December 2021 for pollution owing to discharge of a harmful substance into a river. The second environmental CJIP,[16] dated 18 February 2022, targeted the same type of offence and led to compensation of the ecological damage of €41,925. Transactions on environmental offences are expected to increase in the coming months.

13 AFA, National Multi-Year Plan to Fight Corruption 2020-2022 (January 2020).

14 Law No. 2020-1672 of 24 December 2020 on the European Public prosecutor's Office and Specialised Justice.

15 CJIP No. 21068000009, approved on 16 December 2021.

16 CJIP No. 21179000045, approved on 5 January 2022.

The year 2021 was the first effective year of operation for the European Public Prosecutor's Office (EPPO). Comprising a central college of prosecutors and a network of European delegated prosecutors in every jurisdiction, the EPPO installed delegated prosecutors in France in 2021 to prosecute cases (in the national court system), focusing on the financial interests of the European Union (such as EU subsidies fraud, large cross-border VAT fraud or EU-related bribery).[17] The EPPO confirmed in its first annual report that it had 29 active investigations in France as of December 2021 (out of 515 across the European Union) with estimated total damages to EU funds of €46.1 million.

Highest court continues to refine position on corporate liability

In France, legal persons such as corporations are criminally liable for offences committed on their behalf by their organs (eg, a board of directors) or representatives.

In November 2020, there was a widely publicised Court of Cassation decision that reversed France's position on successor liability. Under previous case law, and in line with the classical French approach assimilating the end of a corporation's legal existence to the death of a physical person, the surviving corporation could not be prosecuted for the offences of the acquired entity (that ceased to legally exist as a result of the merger).

Although it was consistent with fundamental principles of French criminal law, it clashed with the European Court of Justice's view on the matter.[18] The approach adopted in November 2020, which only applies to mergers conducted after the date of the decision, considers that corporations may now be prosecuted for pre-merger criminal conduct of the companies they acquire (ie, criminal liability is passed on to the successor company).

Following the decision, the AFA issued revised guidance on mergers and acquisitions,[19] which confirms the now-established (but not legally mandated) practice of assessing a target corporation's situation in respect of bribery issues for both compliance and possible acts of corruption.

17 For example, bribery involving EU civil servants or officials.

18 European Court of Justice, 5th Chamber, Case No. C-343/13, 5 March 2015, *Modelo Continente Hipermercados SA*.

19 AFA, Practical Guide: Anti-corruption due diligence for mergers and acquisitions (March 2020).

In June 2021, further expanding the possibility of bringing suits against legal entities, the Court of Cassation confirmed[20] the emerging trend of criminally prosecuting the holding company for an offence committed by its subsidiary, despite the above-mentioned obstacles. In this case, employees of the subsidiary were considered as de facto representatives of the holding company – a deviation from previous case law that was deferential to the letter of the law and generally required identifying acts by decision-making organs or individuals formally appointed as representatives of the defendant entity.

Although this decision is not a U-turn, it reflects the French courts' attempts to effectively hold accountable large groups and their parent companies in addition to their subsidiaries for offences committed by the latter. Courts and prosecutors are trying to adapt French criminal law, which does not yet have strict criminal liability tools (eg, failure to prevent bribery-type offences), to the modern corporate reality by pragmatically taking into account group policies and the fact that the corporate structure (ie, holdings and subsidiaries) can sometimes greatly differ from the actual management structure within the organisation.

Impact of internal investigations on CJIP deals

The joint guidelines by the AFA and the PNF issued in June 2019 offered a consolidation of the agencies' doctrines on the prosecution of corruption offences. In the guidelines, the agencies cite the implementation of an effective compliance programme and cooperation of the targeted entity as key factors to reach a CJIP agreement with prosecutors.

Although 'cooperation credit' is not presented as automatic, the agencies explicitly say that cooperation can reduce penalties. They cite self-reporting and cooperation through internal investigations (turned over to the government) as essential factors for the prosecutors not only to decide whether to allow a transactional outcome but also to determine the sentence or fine.

The record-breaking €3.6 billion sanction imposed in January 2020 on an aircraft manufacturer confirmed that French prosecuting authorities and jurisdictions are now a force to be reckoned with in foreign bribery enforcement. This case involved not only government agencies – the French and British authorities formed a joint investigation team – but also an extensive internal investigation.

20 Court of Cassation, Case No. 20-83.098, 16 June 2021.

The agreements – DPAs in the United Kingdom and the United States and a CJIP in France – were discussed at length in the media for the sheer size of the fines imposed. The case highlighted that the PNF's willingness to work on transactional agreements has allowed France to assert its role in French-centric cases where US extraterritorial jurisdiction would have gone unchallenged in the past. It also highlighted the benefits of cooperation efforts by corporations charged with corruption-related wrongdoing.

By conducting an internal investigation of a scale rarely seen in Europe, the company displayed cooperation that was taken into account as a mitigating factor, even though it did not self-report the wrongdoing.

In August 2021, a French company entered into a CJIP that demonstrated the positive outcome that can arise from internal investigations. Following an internal inquiry that uncovered acts of bribery, the corporation self-disclosed to the PNF. The latter was already investigating the company (for other contracts) and reduced the penalty in consideration of the corporation's cooperation efforts.

In February 2022, in cooperation with the PNF, the AFA published a draft guide to internal anti-corruption investigations. It describes the circumstances in which an investigation is warranted, the conditions under which it can be carried out and the consequences to be drawn from an organisational, disciplinary and legal standpoint.

However, despite the guidelines and recent cases presented above, the French regime still does not outline a clear framework for how cooperation credit may be awarded in such cases; at times, cooperating can feel like a leap of faith for corporate defendants who do not know what to expect.

In addition, a crisis of confidence may be looming as prosecutors and practitioners are reminded that judicial approval is a key step of negotiated justice for both corporations and individuals in France.

Since physical persons are ineligible for CJIPs, the fate of directors, officers or employees involved in (or accountable for) wrongdoing has long involved using, after the corporation's settlement, a negotiated procedure offering an agreed-upon sanction in exchange for a guilty plea (CRPC). The two proceedings are, in practice, negotiated at the same time but remain subject to judicial approval and are, in principle, procedurally separate. This means that there is a risk that judges approve the corporation's CJIP but not the CRPC for one or more individuals (which would then be sent to trial, defeating in part the purpose of negotiated proceedings).

This risk materialised for the first time on 26 February 2021, when the Paris Criminal Court approved the €12 million CJIP for a French corporation accused of public agent bribery and fraud in an African country, but declined to approve the proposed sanctions for the CEO and two officers of the corporation (the individuals had agreed to a €375,000 sanction) because they were deemed too lenient.

More recently, in December 2021, this issue occurred again, stress-testing a key aspect of the French regime. The Paris court approved the €10 million CJIP for a French corporation accused of influence peddling in France, but refused to validate the CRPC of one individual involved (who was not a director or employee of the corporate target).

These very public refusal decisions raised an issue practitioners had long been worried about: are faster negotiated proceedings such as CJIPs any use if directors, officers and employees always remain at risk of being sent to lengthy and taxing criminal trial proceedings? Practitioners, prosecutors and legislators (who already started proposing amendments on the issue in recent judicial reform bills) are likely to try to solve this issue in 2022 to maintain the credibility of such proceedings and the attractiveness of the French forum to self-report white-collar matters. This situation could be addressed by a new comprehensive anti-bribery bill that was introduced in Parliament; however, this bill is not yet scheduled for discussion, and this process is expected to take time.

CJIP deal or trial? Courts are still an option to consider

Sapin II's creation of the AFA and its capacity to audit and administratively sanction corporations does not mean that judicial enforcement (ie, by prosecutors, in contemplation of a trial or an agreement when available) is a lesser legal risk.

The past four years have proven that the CJIP procedure is successful. It bolstered the credibility of French enforcement, especially in comparison to the US and the UK systems. It is now systematically considered by professionals in eligible cases, including lower-stakes cases and cases outside of the Paris area that are handled by local prosecutor's offices (eg, a CJIP in Nice in May 2020 for tax fraud and laundering that included a €1.4 million fine).

It seems that judicial white-collar enforcement will get tougher in the foreseeable future, as suggested, in particular, by the €3.7 billion fine for a Swiss bank (2018) and €800 million in damages after it declined a CJIP deal for a smaller amount (€1.1 billion). In December 2021, the Paris Court of Appeal partially overturned this conviction, significantly reducing the fine to €3.75 million (with an additional

confiscation penalty of €1 billion and €800 million in damages to be paid to the state, still making the total amount to be paid one of the most consequential in French judicial history).

The Court of Appeal drastically decreased the amount of the fine because the Court of Cassation ruled in September 2019 that the basis of the proportional fine incurred by the perpetrator of a tax fraud laundering operation needed to be based on the actual tax loss for the state (and not the total taxable sums concealed, which was the base used by the first court in 2018).[21] The Court of Appeal again found the bank guilty and ruled it was not able to calculate a proportional fine using the new method because of 'the indeterminacy of the exact amount of the proceeds of the money laundering'. It therefore defaulted to imposing the maximum discretionary fine for legal entities for this offence – €3.75 million. As is allowed by law, the Court of Appeal also ordered the seizure of €1 billion as proceeds of the offence. A recourse before the Court of Cassation is pending.

This saga shows that in France, despite the success of CJIPs, trial can still be an option to consider in some cases. Counsel and corporate clients should factor in the length, publicity and uncertainty of the trial, as well as the opportunity to get thorough judicial review on key aspects, such as the computation of proportional fines and disgorgements.

Judicial cooperation: towards reform of the French blocking statute?

Heavy fines on French corporations on international sanctions matters (eg, the US$8.9 billion fine for a French bank in 2014) or anti-bribery (eg, the US$772 million fine for a company operating in the transport sector in 2014) based on extraterritorial jurisdiction have become a very sensitive issue in the French political space. The need for more protection of French companies' data and documents has incited the government to act on the issue.

Since 1968, the French have had a blocking statute designed to prevent the abuses of entering into discoveries or subpoenas on French entities or individuals. It criminalises the transmission of information to foreign courts outside the channels set forth by treaties (eg, the 1970 Hague Convention for civil matters or the mutual legal assistance treaties for criminal issues). Although it was applied recently (in an attempt to conduct depositions in the Executive Life case), it is widely considered as not being strictly enforced (notably by the US Supreme Court in its 1987 *Aérospatiale* decision).

21 Court of Cassation, Case No. 18-81.040, 11 September 2019.

After several failed reform attempts by previous legislatures, French MP Raphaël Gauvain was tasked by the prime minister to write a report on measures to limit the impact of extraterritorial assertions of jurisdiction, which included a possible reform of the French blocking statute. The report, which was published on 26 June 2019, proposed, among other things:

- stricter enforcement of the statute, with heightened sanctions in the event of transmission of evidence in civil or criminal proceedings (up to two years' imprisonment and a €2 million fine for physical persons and €10 million for legal entities);
- administrative sanctions of up to €20 million for physical persons and up to 4 per cent of the global turnover for legal entities (eg, cloud service providers) that unlawfully transfer data abroad in anticipation of litigation – this provision aims to limit the extraterritorial effects of the US CLOUD Act and its coercive power on French or European companies; and
- mandatory registration with the Ministry of Economy's economic intelligence office (SISSE) of corporations targeted by foreign investigations – the government may directly conduct the dialogue itself in certain important cases where strategic issues are at stake.

In 2022, rather than opting for a bill and increasing penalties in the event of a violation of the blocking statute, the government chose to clarify the reporting process via a decree enacted in February, followed by a regulation in March. The decree indicates that companies receiving requests that may fall within the scope of the blocking statute must inform the SISSE.

In practice, a filing must be submitted to the SISSE, which has one month to reply regarding the applicability of the blocking statute. The violation of the obligation to report to the SISSE is not sanctioned by any specific penalty.

Although these 2022 amendments help identify the relevant agency, it does not make the incurred penalties higher, nor does it substantially change how the law is enforced. For these reasons, these technical changes alone are unlikely to change the current position of foreign courts when assessing the credibility and actual enforcement risk of the French blocking statute.

In parallel with these French developments, EU-level solutions are also in the works.

EU projects, including the upcoming e-evidence regulation, are intended to pursue this effort and offer a common defence of EU companies and data while still providing a framework for cooperation against crime. Trilogue negotiations on this regulation started in February 2021 between the European Parliament, the Council and the Commission.

Following its experience with Sapin II, France is spearheading an EU-level push to adopt common legislation on the detection and prevention of corruption. This may imply a new role for the EPPO, which started its operations in June 2021 and is, for now, an independent prosecution body focused on defending the financial interests of the European Union across its member states' courts.

Duty of Vigilance Law now EU-wide?

Enacted on 27 March 2017, the Duty of Vigilance Law is France's initiative to promote the accountability of large corporations regarding the prevention of ESG risks related to their operations (including their subsidiaries and business partners, such as subcontractors or suppliers).

Although norms on this topic, such as the UN Guiding Principles on Business and Human Rights of 2011, have long remained non-binding soft law, France's initiative was original as it initiated a 'hardening' of human rights obligations for businesses.

The Law applies to companies with at least 5,000 employees within their company and in their direct and indirect subsidiaries when their registered office is in France, and 10,000 employees when their registered office is located abroad. This includes French subsidiaries of foreign companies or global groups insofar as they meet the above-mentioned requirement.

The 'vigilance plan' is the key measure of the Duty of Vigilance Law, requiring qualifying companies to set up a plan containing measures designed to identify and prevent risks of human rights violations, serious physical or environmental damage and safety risks.

In line with the spirit of the Sapin II-mandated compliance plan for bribery, the vigilance plan must cover items such as:

- risk mapping;
- procedures for evaluating subsidiaries, subcontractors and suppliers with whom an established commercial relationship is maintained;
- appropriate actions to mitigate risks or prevent serious violations;
- a mechanism for alerting and collecting alerts; and
- a mechanism for monitoring the measures implemented to assess their effectiveness.

The plan must be published in the corporation's annual report, which can be enjoined to establish and publish a plan if it fails to do so. [22]

In the past few years, NGOs have actively tracked qualifying corporations' compliance with the law,[23] and proceedings were initiated in 2019 against a French oil company, alleging insufficiencies in the vigilance plan regarding extraction operations in Uganda and pursuing – as a first remedy – an injunction to correct the plan.[24] The case hit a procedural roadblock on 30 January 2020 as the Nanterre Civil Court declined jurisdiction in favour of the commercial court, which plaintiffs consider less likely to support their case. On 10 December 2020, the Versailles Court of Appeal confirmed the decision and the jurisdiction of the Nanterre Commercial Court.

According to a January 2020 government report citing external studies,[25] some eligible corporations are not yet compliant with the law, exposing themselves to major liability and damages if an incident happens.[26]

Failure to comply with the law (ie, to effectively implement the plan described above) exposes the corporation to a new form of fault-based civil liability in the event of an incident, where it can be liable for damages 'repairing the harm that [its] compliance with the law could have avoided'.[27] This means that, although the occurrence of an accident in a subsidiary or subcontractor does not necessarily mean that the corporation is liable (as a fault is required), companies are bound by a duty of care that comprises thoroughly implementing the vigilance plan.

The very broad writing of the law means that only the first liability cases will allow us to grasp its real extent and assess whether it reached its goal to foster accountability without creating an overly burdensome liability regime. To date, few proceedings were initiated,[28] and no decision on the merits has been handed down in France.

---

22 As the sanctions originally present in the law were declared unconstitutional.

23 See, for example, the 'Duty of vigilance radar' (https://plan-vigilance.org/) created by three NGOs.

24 For context, see, for example, 'Campaign groups accuse Total of breaching French corporate duty law in Uganda', *Reuters* (25 June 2019).

25 A Duthilleul and M de Jouvenel, report to the Ministry of the Economy, 'Implementation assessment of Law No. 21017-399 dated 27 March 2017 on the duty of vigilance of parent companies' (January 2020), page 28.

26 id, page 30.

27 Article 225-102-5 of the Commercial Code.

28 A recent parliamentary report (C Dubost and D Potier, Report on the assessment of the 27 March 2017 on the duty of vigilance (24 February 2022)) lists a total of six cease-and-desist letters for non-publication of a plan, four injunction requests and a single liability action. None have led to a definitive decision so far.

France, whose approach to ESG issues through 'hard law' was at first isolated among the EU member states, was followed by Germany in June 2021. Besides differences with France in terms of the scope and the due diligence requirements under the German Duty of Vigilance Act, the main discrepancy concerns enforcement: in Germany, non-compliant companies face the risk of being excluded from public contracts for up to three years and fines of up to 2 per cent of their global annual turnover.

In February 2022, after public consultation, the European Commission proposed, in February 2022 a directive on corporate sustainability due diligence that would set an obligation for corporations to perform due diligence on human rights and environmental risks. Administrative authorities designated by each member states would be in charge of imposing fines in the case of non-compliance, perhaps curing some of the enforcement deficiencies observed in France, and victims would have the right to take legal action against such companies for 'damages that could have been avoided with appropriate due diligence measures'.

* *The authors wish to thank Matthieu Delignon for his contribution to this article.*

LUDOVIC MALGRAIN
White & Case

Ludovic Malgrain is a partner in the white-collar crime and regulatory group of White & Case in Paris. He has been a member of the Paris Bar since 1998 and has developed a recognised expertise in criminal defence. He is regularly ranked as a leading criminal defence lawyer in France by leading directories.

Ludovic represents French and international high-profile clients, corporate entities and individuals, within the industrial, oil and gas, banking and technology sectors before French authorities, agencies and courts. He is able to represent and advise clients on all types of criminal offences, such as embezzlement, fraud, workplace accidents and moral harassment.

In particular, the team handles cases connected to fraud or allegations of bribery in Angola and Nigeria, tax fraud through schemes in Luxembourg and Switzerland, market abuse for listed companies and commercial malpractice in the banking and consumer sectors. In addition, the team provides assistance in internal and multi-jurisdictional investigations (US Department of Justice, UK Serious Fraud Office, etc). Ludovic has strong expertise assisting companies in the context of administrative controls launched by the French Anti-Corruption Agency in relation with the Sapin II law.

Backed by 20 years of hands-on litigation experience in international law firms, Ludovic offers guidance to satisfy legal requirements relating to prevention of corporate criminal liability for managers and corporations as well as implementation of compliance programmes (anti-bribery, anti-money laundering, etc).

His track record includes a number of high-profile cases, such as the collapse of the gangway of the Queen Mary II passenger ship, the Air France Concorde crash, the EC Eurostat scandal, the *Apollonia* fraud, the *Helvet Immo* class action and the *Dubai Papers* case.

JEAN-PIERRE PICCA
White & Case

Jean-Pierre Picca is a partner in the white-collar crime and regulatory group of the Paris office. A senior legal adviser to the president of the French Republic between 2010 and 2012 as well as senior prosecutor, Jean-Pierre held a variety of high-level duties within the French judiciary before joining the firm.

He notably performed functions as a senior liaison legal adviser to the US Department of Justice between 2002 and 2007. Jean-Pierre has 30 years of experience in the criminal area both as a prosecutor in France and in the United States and as a defence lawyer. He was involved in landmark cases such as the *Concorde* crash, the *Executive Life/Crédit Lyonnais* matter and the criminal investigations in the aftermath of the 9/11 terrorist attacks.

Jean-Pierre has been at the forefront of headline financial investigations and crossborder complex litigation, advising several leading French banks in major investigations driven notably by the French and US authorities. He has acquired an in-depth knowledge of strategic issues and frequently advises senior management of his clients.

He has represented both companies and individuals in the course of major international sanctions cases. He is also deeply involved in the context of the EURIBOR/LIBOR investigations alongside a major international bank. He regularly advises a major private equity fund on several aspects: anti-corruption, criminal investigations, transfer and sale of shares. Jean-Pierre also assists several clients on complex compliance issues (governance and compliance with AML regulations in France and abroad). He has recognised skills in crisis management and complex cross-border disputes.

GRÉGOIRE DURAND
White & Case

Grégoire Durand is an associate in the white-collar practice of White & Case in Paris. He advises financial institutions, major corporations and individuals on domestic and cross-border criminal fraud and contentious regulatory matters.

His practice includes representing clients in relation to criminal banking litigation, fraud, money laundering, bribery and criminal aspects of consumer law.

Grégoire is a graduate of Sciences Po Law School and the University of Chicago Law School. He is admitted to practise in Paris and New York.

WHITE & CASE

Our global white-collar and investigations team regularly handles a wide range of complex, high-stakes and multi-jurisdictional legal matters. We address the risks and complexities arising from investigations and enforcement actions. With our global footprint, experience and skill, we provide comprehensive and cost-effective representation and advice to clients facing exposure to civil and criminal liability.

Our team in Paris offers first-rate expertise in advising and defending clients through all phases of global investigations, as well as criminal proceedings, antitrust investigations and contentious regulatory disputes. Our team is over 35 lawyers strong and growing.

We have substantial experience in dealing with multi-jurisdictional investigations carried out by French, European and foreign jurisdictions or regulatory and control authorities and have acquired in-depth knowledge of international judicial process and procedures.

In addition to our broad experience and technical expertise, we have assisted clients with matters involving the European Commission; the Financial Markets Authority, the Prudential Control Authority, the French Medicinal Security Agency and the Competition Authority in France; the Financial Conduct Authority and Serious Fraud Office in the United Kingdom; the Department of Justice, the Department of Financial Services and the Commodity Futures Trading Commission in the United States; as well as the Japan Financial Services Authority and Monetary Authority of Singapore in Asia.

We work closely with our colleagues from our offices around the world, in particular in Brussels, Washington, DC, New York, London, Tokyo, Singapore and Hong Kong, and regularly field cross-practice teams including experts in data protection, bank supervisory, capital markets and tax.

19 Place Vendôme
75001 Paris
France
Tel: +33 1 55 04 15 15
www.whitecase.com

Ludovic Malgrain
lmalgrain@whitecase.com

Jean-Pierre Picca
jppicca@whitecase.com

Grégoire Durand
gregoire.durand@whitecase.com

Corporate Criminal Liability under Italian Law

Roberto Pisano
Studio Legale Pisano

IN SUMMARY

The 2001 law regarding corporate criminal liability significantly affected the practice of criminal lawyers in advising corporate entities and their strategy for criminal investigations and prosecutions. Companies can be considered liable in respect of a wide range of criminal offences committed by their managers or employees in the interest or for the benefit of the company. A company's liability is qualified by the law as an administrative offence that involves not having implemented an adequate compliance programme that is able to prevent the commission of the criminal offence by its managers or employees. Where the criminal offence is committed by senior managers, the liability of the company can theoretically be avoided; however, the standard of proof is extremely high and almost unreachable in practice.

DISCUSSION POINTS

- Nature and requirements of corporate liability
- Applicable procedure
- Conditions to exclude or mitigate corporate liability
- Applicable sanctions

REFERENCED IN THIS ARTICLE

- Legislative Decree No. 231/2001
- Court of Cassation, United Sections, 24 April 2014, No. 38343
- Code of Criminal Procedure
- *Impregilo*
- *Siemens AG*

Fundamental principles of corporate criminal liability

As of 2001, companies can be considered criminally liable with regard to a list of criminal offences committed by their managers or employees in the interest or for the benefit of the company (Legislative Decree No. 231/2001 (Law 231)).

The list of predicate offences is constantly updated and broadened. It currently covers a wide range of business crimes, such as corruption, tax fraud and fraud against the state, market manipulation and insider trading, false accounting, money laundering, handling stolen goods, health and safety crimes, intellectual property crimes, infringement of trademarks and environmental crimes.

A company's liability is qualified by the law as an 'administrative offence' that comprises not having implemented an adequate compliance programme or internal control system that is able to prevent the commission of the criminal offence by its managers or employees; however, the competence for the investigation and prosecution of a company's offences lies with the ordinary prosecuting authorities, in accordance with the rules of criminal procedures and in the frame of criminal proceedings subject to the jurisdiction of criminal courts, which are usually joined with the criminal proceedings against the managers or employees who committed the predicate offence.

Case law on this is consolidated in the sense that the corporate liability has the nature of criminal liability, with the consequence that all related principles and guarantees provided for by criminal law (ie, personality of criminal liability) must be applied.[1]

Fundamental principles of criminal procedure

In the Italian legal system, public prosecutors are responsible for the investigation and prosecution of all criminal offences, including business crimes, of both individuals and companies. They are assisted by the police.

Public prosecutors are not part of the government but are professional magistrates, such as court judges, and their decision to bring criminal prosecutions is compulsory not discretionary. This means that when they acquire or receive a 'notice of crime' – a notice regarding specific facts potentially constituting a crime – they have a duty to open formal criminal proceedings (by immediately registering the notice in a special register) and start an investigation. Subsequently, if they assess that an offence was committed by certain individuals or companies, they have a duty to bring a criminal prosecution by requesting the committal for trial of the targets.

1 Court of Cassation, United Sections, 24 April 2014, No. 38343.

The investigation does not start if the event to which the notice refers is clearly unable to constitute a criminal offence (including a company's offence). In any case, where public prosecutors assess that the notice of crime is ungrounded, they have the power to directly dismiss the case with regard to companies, although with regard to individuals they must request the dismissal to the competent judge (the judge for preliminary investigations).

The notice of crime can be generated from multiple sources, such as criminal complaints filed by injured parties; reports made by the police, other public officials or the relevant enforcement agencies (eg, tax authorities or the authority regulating the financial market, Consob); or other channels, such as press articles.

The acts of investigation carried out by the public prosecutors with the assistance of police officers are, with some exceptions, covered by judicial secrecy until the conclusion of the preliminary investigations. The time limit for carrying out and concluding the preliminary investigation is six months, extendable up to a maximum of two years (and even longer if new suspects are added to the original investigation).

Once the time limit has been reached, the individual and companies under investigation are entitled to obtain a copy of all the acts of investigation (articles 329 and 415-bis of the Code of Criminal Procedure (CCP)), and in the subsequent 20-day period, they have the right to request to be interviewed by the public prosecutor and to file written submissions to convince the prosecutor's office not to request the committal for trial.

The existence of a criminal investigation is usually publicly acknowledged at an earlier stage than the conclusion of the investigation, especially when peculiar acts of investigation are carried out, such as the execution of search and seizure or the issuance of arrest warrants. Individuals or companies that are potential targets of a criminal investigation have the right to file a formal application to the public prosecutor to be informed about their status as persons under investigation. Under specific requirements, the public prosecutor can deny disclosure for a limited period.

Conditions for excluding corporate criminal liability

On the basis of Law 231, companies can be considered criminally liable for the offence of not having implemented an adequate compliance programme or internal control system that is effectively able to prevent criminal offences by their managers or employees, in respect of a compulsory list of criminal offences committed by their managers or employees, in the interest or for the benefit of the company (article 5 of Law 231).

Where the predicate criminal offence is committed by an employee, the company can avoid liability by proving that it has implemented an adequate compliance programme that is properly designed to effectively prevent the commission of that type of offence (article 7).

Where the offence is committed by senior managers, however, the liability of the company can be avoided only by proving that:

- the company has implemented an adequate and effective compliance programme;
- there was sufficient surveillance by the supervisory board (ODV); and
- the senior manager committed the offence by 'fraudulently circumventing' the mentioned corporate internal controls (article 6).

In this scenario, a crucial role is performed by the ODV, which has the fundamental function of monitoring and continuously supervising the effectiveness and adequacy of the compliance programme or internal control system of the company for the purpose of excluding or mitigating corporate criminal liability. In particular, to be excluded from liability or leniency, the ODV must be composed of qualified professionals and have, and effectively exercise, autonomous powers of action that are independent from those of the management (and other corporate bodies).

However, according to Italian case law, where the predicate criminal offence was committed by a senior manager, the standard to prove that the compliance programme in place and the surveillance by the ODV were totally adequate and effective, and that the perpetrator acted by fraudulently circumventing the mentioned internal controls, is extremely high and almost unreachable in practice.

A violation by a senior manager of the principles, policies and procedures imposed by the compliance programme is not sufficient to obtain an acquittal: the company has the burden of proving that an effective fraud of the internal control system was performed by the senior manager, who was effectively able to mislead the other officers and bodies of the company in such a way as to prevent a perfect internal control system from detecting and impeding the violation.[2]

Such a standard is extremely difficult to meet and almost unreachable in practice. There have been several requests and proposals for change by scholars and the business community.

2 Court of Cassation, section V, 18 December 2013, No. 4677, *Impregilo*.

Sanctions

Sanctions applicable to companies under Law 231 include fines, disqualifications and confiscation of the proceeds of crime (article 9).

Fines always apply in the event of a company's conviction. Their financial impact does not usually exceed €3 million, and it is often lower depending on several factors, such as the type and seriousness of the offence, the degree of liability of the company, the activity carried out by the company to eliminate or reduce the consequences of the offence and prevent the commission of further offences, and the economic and patrimonial conditions of the company (articles 10 to 11).

Disqualifications can include:

- suspension or revocation of government authorisations, licences or concessions;
- debarment (prohibition of entering into contracts with the public administration);
- exclusion from or revocation of government financing, contributions or subsidies; and
- prohibition from carrying on business activity.

Disqualifications compulsorily apply in the event of conviction of the company, where the following requirements are met:

- the criminal offence was committed by a senior manager or by employees and in the latter case the commission of the offence was a result of serious organisational deficiencies; and
- the company has obtained 'significant profits' as a result of the crime committed by its managers or employees (article 13).

Disqualifications compulsorily apply in the event of reiteration of the company's offence. Reiteration occurs where the company commits an offence in the five-year period subsequent to its res judicata conviction for a previous and different offence (article 20).

Disqualifications can be particularly damaging, and this is amplified by the fact that they can also be applied at a pretrial stage, during the investigations, as interim coercive measures (article 45).

The application of interim coercive measures, such as disqualifications, is ordered by the judge for preliminary investigations on request of the public prosecutor, where the following requirements are met:

- there is serious evidence of a company's commission of an offence;
- there is concrete risk of commission of further offences (of the same type as the ones under investigation); and
- the company has obtained 'significant profits' as a result of the crime committed by its managers or employees.

An advisable strategy to reduce the risk of a company being subject to interim coercive measures is to eliminate the risk of commission of further offences. Where there appears to be prima facie grounds for criminal investigation, it is advisable to react to the knowledge of it by immediately adopting appropriate and effective reaction measures, such as:

- suspending working relations with and revoking the powers of the managers or employees who are alleged to have had a key role in the criminal activity;
- entrusting a qualified forensic firm to carry out an in-depth assessment of the allegations and the effectiveness of the company's internal control system, with the task of identifying any possible gaps and advising on improvements; and
- presenting to the prosecuting and judicial authorities an effective remedial plan to be promptly implemented.

Leniency and cooperation with the authorities

The Italian system does not provide for a formal mechanism by which companies can cooperate with the investigation or disclose violations in exchange for immunity or lesser penalties (with the exception of plea bargaining); however, a certain degree of cooperation with the prosecuting authorities during the investigations and before trial can have a significant impact on reducing the pretrial and final sanctions imposed on the company.

In particular, applicable fines can be reduced by up to two-thirds, and disqualifications can be excluded if the following conditions are fulfilled before the opening of the trial of first instance is declared:

- the company has entirely compensated damage and eliminated the damaging consequences of the crime, or has taken effective actions in that respect;
- the company has eliminated the organisational deficiencies that generated the crime by adopting and implementing an adequate compliance programme that is able to prevent the commission of offences of the same type as those under investigation; and
- the company has made the profits obtained from the crime available to the authorities for confiscation (article 17).

It is generally advisable to adopt appropriate and effective reaction measures as soon as the investigation is known about, and ensure they are entirely executed before the deadline provided for by the law in order to benefit from leniency (ie, the declaration of opening of the trial of first instance).

Under certain conditions, plea bargaining with prosecuting authorities is recognised by Italian law, both for individuals and companies.

As far as individuals are concerned, the plea bargain must be approved by the competent judge. The punishment agreed with the prosecution's office cannot be more than five years' imprisonment, and it is considered equivalent to a conviction by an express law provision (article 444 of the CCP). The adoption of plea bargaining entitles the offender to a reduction of the punishment by up to one-third.

In respect of companies, a similar mechanism of plea bargaining is available in relation to less serious offences and to predicate criminal offences for which the managers or employees under investigation are entitled to a plea bargain (article 63 of Law 231). The reduction of the sanctions by up to one-third owing to plea bargaining also applies, and the reduction operates on the amount of the fine and on the length of the relevant measure of disqualification.

Even if the plea bargain is considered equivalent to a conviction by an express law provision, an admission of wrongdoing is not required. In particular, according to case law, a plea bargain cannot be considered an admission of wrongdoing, but rather as an incomplete assessment of liability deriving from the decision of the defendant to renounce challenge of the charges.

In the related civil litigation, the plea bargain is not binding on the civil judge as a conviction issued after a full trial would be; however, it has the value of ordinary evidence that can be evaluated by the civil court.

A conviction of the company for offences under Law 231– and, under certain conditions, a plea bargain – may remove the ability of the company to take part in public tenders.

Jurisdiction of Italian courts and liability under Law 231

The main governing principle of the jurisdiction of Italian courts, in respect of both individuals and companies, is territoriality, according to which Italian courts have jurisdiction on all offences considered to be or have been committed within Italian territory. This principle suffers derogation in favour of extraterritorial jurisdiction only to a very limited extent and under stringent requirements.

The principle of territoriality is interpreted in a broad sense with a wide reach since it is sufficient that only a portion of the prohibited conduct took place in Italy for it to be under Italian jurisdiction; therefore, foreign companies that have their registered seat and main place of business abroad can be subject to Law 231 and be prosecuted in Italy if at least a portion of the criminal offence committed by their managers or employees took place in Italy and all the other requirements for the company's liability are fulfilled.

In essence, the predicate offence must have been committed in the interest or for the benefit of the foreign company by its managers or employees, and the foreign company should have failed to implement an adequate and effective compliance programme to prevent the commission of the offence.

The principle of the liability of foreign companies under the strict terms mentioned previously (with a corresponding burden to adopt a compliance programme in accordance with the principles of Law 231, where the companies are conducting part of their business in Italy) is consolidated in Italian case law – ever since the landmark decision *Siemens AG*.[3]

In respect of companies that have their main seat (registered office or main place of business) in Italy, including Italian subsidiaries of multinational groups, the jurisdiction of Italian courts applies not only with regard to offences committed in Italy but also under stringent conditions (including the fact that the offence is not prosecuted in the foreign state of commission), in relation to offences committed abroad (article 4 of Law 231); therefore, in that limited respect, the principle of territoriality suffers derogation in favour of extraterritorial jurisdiction.

Law 231 does not provide for any express provision to regulate corporate liability in a group of companies. The most significant issue, in particular, is whether a parent company can be held responsible under Law 231 in relation to a criminal offence committed in the immediate interest or for the benefit of its subsidiary.

According to the prevailing case law, the answer is negative: a holding or parent company can be responsible under Law 231, but only if the relevant law requirements are satisfied. In particular, a manager or employee of the parent company must be involved in the commission of the predicate criminal offence, and the predicate criminal offence must have been committed in the specific interest or for the specific benefit of the parent company.

In other words, it is not admissible to infer an interest or benefit for the parent company only on the basis of the group relation because this conflicts with the fundamental principle of personality of criminal liability.[4]

---

3 Milan Judge for Preliminary Investigations, 28 April 2004; subsequently confirmed by the Court of Milan, 28 October 2004.

4 Court of Cassation, Section IV, 18 January 2011, No. 24583; Court of Cassation, Section II, 27 September 2016, No. 52316; and, in a contrary and broader sense, Court of Cassation, Section III, 11 January 2018, No. 28725.

ROBERTO PISANO
Studio Legale Pisano

Roberto Pisano is the founder and managing partner of Studio Legale Pisano. He has a history of representing prominent individuals and entities in high-profile Italian criminal investigations and trials with media impact, including various cases of corruption involving international corporations and their top officials (with multiple investigations in the United States, the United Kingdom, France, etc); various cases of extradition, including the *FIFA* investigation and representation of foreign states; three cases of alleged tax fraud involving the former Italian prime minister; a case involving a major US bank in the bankruptcy of the Parmalat group; a case involving a claim for restitution of antiquities by the Italian Ministry of Culture against a prominent US museum; various appeals in foreign jurisdictions (eg, the United States, Hong Kong, Switzerland and Monaco) against freezing and confiscation of assets; and Italian criminal counsel for foreign multinationals and Italian companies conducting internal investigations. Pisano also advises and represents relevant foreign governments.

Pisano obtained a law degree, summa cum laude, from the State University of Milan in 1992 and a PhD from the University of Genoa in 1999. He was co-chair of the business crime committee of the IBA in 2007 and 2008 and vice chair of the ECBA in 2008 and 2009. He is the author of several publications on the subject of business crime and mutual legal assistance.

Studio Legale Pisano

Studio Legale Pisano is an Italian boutique firm that specialises in all areas of white-collar crime, including corporate criminal liability, corruption, market abuse and false accounting, tax crimes, money laundering, fraud and recovery of assets, bankruptcy crimes, and environmental and health-and-safety crimes. Since 2007, the firm has provided assistance in the course of criminal and regulatory investigations and specialises in transnational investigations and related aspects of mutual legal assistance and extradition.

Studio Legale Pisano benefits from the expertise of specialists in criminal and international law and interacts daily with counsel of various jurisdictions. The firm has a history of representing prominent individuals and entities in high-profile Italian criminal investigations and trials, in extradition proceedings and in the frame of foreign proceedings for judicial review of search and seizure and freezing orders. The firm also represents and advises foreign governments on issues of international criminal law and in extradition proceedings, and carries out internal investigations on behalf of foreign multinationals and Italian companies.

Via Cino del Duca 5
20122 Milan
Italy
Tel: +39 02 7600 2207

Roberto Pisano
robertopisano@pisanolaw.com

A Booster Shot of Compliance for Companies in Central and Eastern Europe

Bogdan Bibicu, Jitka Logesová and Jaromír Pumr
Wolf Theiss

IN SUMMARY

The increased focus of companies in Central and Eastern Europe (CEE) in tackling large-scale corruption through corporate criminal liability has resulted in an increasing number of companies being prosecuted each year. Companies have, therefore, been paying closer attention to their compliance efforts. This article discusses the influence of the covid-19 pandemic on the shifting focuses of prosecuting authorities in the CEE region, the compliance status of companies and corporate investigations, and provides an outlook on the future.

DISCUSSION POINTS

- States' shopping sprees for medical devices during the pandemic
- Influence of the pandemic on corporate investigation and compliance processes
- Digital corporate investigations and internal policies for digital-age compliance
- Zero-based redesign of the compliance management system
- Commencement of activity of the European Public Prosecution Office
- War in Ukraine and further related shifts

REFERENCED IN THIS ARTICLE

- Association of Certified Fraud Examiners' report 'Fraud in the Wake of COVID-19: Benchmarking Report'
- US Department of Justice's 'Evaluation of Corporate Compliance Programs'
- Group of States against Corruption
- OECD working groups on bribery and non-trial resolutions
- European Commission's reports on anti-corruption matters

Common ground in the CEE region

The region of Central and Eastern Europe (CEE) is a unique place that stands out owing to its rich tapestry of languages and its abundance of cultures – each embedded in national histories vastly different from one another. This contrasts with the closeness kept by a few groups of nations that share substantial parts of their histories (eg, Slovakia and the Czech Republic – formerly Czechoslovakia).

The legislative and legal landscape of CEE countries and their approach towards compliance is also influenced by each of their current political affiliations. The concept of corporate criminal liability is still a relatively new concept for many white-collar crime practitioners and prosecuting authorities in CEE countries. The concept more or less followed the concept of individual criminal liability, which has created room for many difficulties in application.

Most CEE jurisdictions either allow companies to release themselves from criminal liability if they prove that they have an effective compliance management system (CMS) in place that is able to prevent the investigated criminal behaviour, or consider an effective CMS as a mitigating circumstance for which the company must react with zero tolerance to non-compliant behaviour. Having an internal process in place to investigate non-compliance is understood to be a part of any effective CMS.

For example, in the Czech Republic, companies can release themselves from criminal liability if they prove that they have adequate measures (an effective CMS) in place that could have prevented the crime. In September 2018, non-binding internal guidelines – later modified in 2020 – for Czech public prosecutors were issued. This is relatively atypical for the CEE region. The guidelines were inspired by international guidelines, such as those by the US Department of Justice (DOJ), the UK Bribery Act guidelines and the compliance standards ISO37001 and ISO19600, and are in the form of an internal document that is intended to be used as non-binding guidelines by public prosecutors.

The investigation process in each CEE country is unique, and cross-border investigations across several European jurisdictions have often presented an array of practical challenges. However, thanks to the decades of work put in by the European Union, the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe, a clear trend is becoming apparent in which divergencies can be converged, and multi-jurisdictional corporate investigations or compliance audits can be conducted more easily than ever before.

Unfortunately for some companies, this does not only apply to corporate investigations and compliance audits; law enforcement authorities are also actively cooperating with each other much more frequently and much more swiftly, with this cooperation also extending abroad to their counterparts in jurisdictions such as the United States, the United Kingdom, France, other EU countries and Canada, among others.

Anti-corruption, anti-terrorist financing, anti-money laundering and foreign tax evasion efforts have also started to improve in terms of both the quantity and quality of enhanced coordination and communication at the multi-jurisdictional and global levels. As a result, there is an increasing number of local and multi-jurisdictional corporate investigations that have been triggered by vigilant companies that are highly observant of any signs of non-compliance that could trigger, for example, an investigation in respect of the Foreign Corrupt Practices Act (FCPA), the UK Bribery Act or the French Sapin II should the CEE authorities open an investigation and request information from their foreign counterparts.

This makes sense as companies are handsomely rewarded with significantly milder repercussions – under, for instance, the FCPA by the DOJ – if they detect misconduct early and if they investigate and report their findings to the DOJ.

At present, there are no practical out-of-court solutions in the CEE countries once a company is investigated or prosecuted. Unless the charges are dropped by the prosecuting authorities, the company faces lengthy prosecution in public proceedings. Nevertheless, discussions and proposals around structured settlements, non-trial resolutions and other tools available in other jurisdictions have commenced.

The growing vigilance of companies is accompanied by increased interest among CEE authorities in investigating and prosecuting companies, which is a trend that started more than 10 years ago when CEE jurisdictions, pushed by the OECD and its Working Group on Bribery,[1] the Council of Europe's Group of States against

1 For example, its report on the Czech Republic highlighted that the relatively recently enacted corporate criminal liability and the increasing prosecution of companies was showing promising results, and that increasing international cooperation and joint-investigation teams were signs of good practices. (Available at 'Czech Republic - OECD Anti-Bribery Convention – OECD'). Similar highlights can also be found in respect of other countries, such as Austria (see 'Austria - OECD Anti-Bribery Convention') and Poland (see 'Poland: Follow-up to the Phase 3 Report & Recommendations'). Progress in other states (eg, Romania and Bulgaria) has also been noted (eg, in reports issued by the European Commission).

Corruption or the European Commission, started to focus on corruption by also implementing and pursuing corporate criminal liability, not only individual criminal liability.

It took some time before prosecuting authorities turned their attention towards companies. Nowadays, it may at times be increasingly difficult to lead multi-jurisdictional investigations while satisfying all the relevant countries' laws and to make sure that the company is not punished twice for the same crime. This is one reason for which there is more and quicker cooperation between judicial authorities in different states.

To some extent, this trend was slowed down by the covid-19 pandemic and related local restrictions. The pandemic compelled several countries in the CEE region to, among other things, close their doors to their neighbours, except for essential travel; declare a state of emergency; and shift their attention towards domestic concerns.

Although this trend may have slowed down at a 'formal' level, prosecuting authorities are nonetheless becoming more and more digitally savvy and are developing their IT capabilities, thus enabling them to investigate and communicate on an informal basis while waiting for the formalities to be completed – a process that can be enormously lengthy. This trend is expected to continue despite the recent war in Ukraine, during which the focus may appear to have been shifted more to the war and its immediate local, neighbouring and trickle-down effects.

This article discusses the influence of the covid-19 pandemic on the shifting focuses of prosecuting authorities in the CEE region, the compliance status of companies and corporate investigations, and offers a brief outlook on the future. This article was also based on results in the new edition of the 'Wolf Theiss Guide to Corporate Investigations in Central, Eastern and Southeastern Europe', which addresses corporate investigation matters in detail in individual countries.

State-of-emergency bonanza

As soon as the covid-19 pandemic hit the CEE region, national governments declared states of emergency, arguing that a general lockdown was needed and that certain items and services needed immediate, non-tendered purchasing. The demand for medical supplies (face masks, gloves, ventilators, hospital beds, intensive care supplies, covid-19 tests, laboratory supplies and hospital infrastructure) and services (including non-medical related services) skyrocketed, at one time peaking by several thousand percentage points.

Public procurement contracts also soared in number, many of them deviating from standard procedure and failing to apply appropriate (or any) checks. This simplification (or inobservance) of the public procurement process has also resulted in governments hand-picking their contractors without public bidding or other competitive procedures.

Most governments kept the state of emergency or similar measures in place even after the markets in those items had soared. This led to price hikes, the development of a huge resellers' market and a number of scandals where governments used the covid-19 pandemic as an excuse to justify buying massive quantities of low-quality items from shell companies affiliated with public servants, overlooking local distributors in the process.

For example, the Czech government paid more than US$10 million to a shell company connected with money laundering schemes.[2] The Supreme Audit Office of the Czech Republic, which audited most of the transactions, noted: 'Purchases of protective equipment were accompanied by chaos, significant price differences, shortcomings in their quality, and transportation issues.'[3]

A similar situation arose throughout the CEE region: in Romania, several similar reports have been issued, and similar cases are being investigated by the authorities, including by prosecutorial bodies. In Ukraine, authorities have been able to deal directly with suppliers without going through the federal procurement system Prozorro, although it is suspected that this streamlining may have resulted in abuses of procurement procedures during the pandemic.

In Serbia, a purchase of medical supplements for approximately €10 million was executed without a public tender. The Ministry of Health approached a small number of bidders on its own initiative, and the contract was awarded to a pharmaceutical company whose management allegedly has close ties with the current ruling political elite.

Czech Members of Parliament have already set up a parliamentary commission for investigating government spending during the state of emergency, which could amount to US$1 billion over the year of its duration.

2 Sabina Slonková, 'Nákup testů do škol: podezření z praní špinavých peněz', *Neovlivní* (20 February 2021).

3 Supreme Audit Office of the Czech Republic, Data Annex to Audit Report No 20/32.

In several CEE countries, there have been parliamentary commissions or other processes for investigating government spending during the pandemic or similar periods, which could amount to billions of euros. Moreover, a stringent review is ongoing into the compensation paid to companies during the lockdowns, penalising companies for any mistakes they made and often reclaiming the compensation.

As countries have gradually emerged from lockdown and restrictions have been eased, many companies – particularly in the European Union – are readying themselves to pick up the crumbs of the massive €1.8 trillion recovery fund and NextGenerationEU programme, which will be used to reignite the European economy through public grants to fund modernisation, innovation and environmental protection. Since, in the CEE countries that are EU member states, the focus of local prosecution authorities and the focus of the European Public Prosecution Office on areas involving EU and public funds and related subsidies and public tenders is a priority, companies must ensure that they stay compliant.

The lack of visible enforcement in certain cases does not mean that prosecutorial investigations are not being carried out. As seen from previous economic crises, there are delays between the occurrence of EU and public-related fraud and the time the prosecutorial investigations become visible. The current war in Ukraine is also likely to increase some delays in at least some countries. Proactive internal checks by companies in investigating the relevant pandemic period is far more preferable to limit pending higher risks than addressing a crisis in the upcoming months or years.

Is compliance immune to covid-19 or war?

As the impact of the covid-19 pandemic continues to affect economies, companies and their management have been focusing on how to survive in the short term. A similar reaction is being seen in response to the war in Ukraine. Some areas of business have been clearly struggling to stay afloat or have had to cope with severe disruption, whereas others have been experiencing rapid growth in their operations and sales.

Overall, 'business-first' logic seems to rule the roost, and the mantra of 'no time for compliance' has – unfortunately – been increasingly applied; however, even where the situation is desperate, the ends do not justify the means. Criminal activity is no less prohibited, and a state of emergency makes the consequences more, not less, severe.

Although government authorities may appear to be busy dealing with more urgent matters (eg, the war in Ukraine), prosecuting authorities are active in investigating crimes pertaining to the pandemic. Some of those authorities are now more experienced and more equipped than they had been during economic crises that generated more non-compliance.

Not only were most businesses affected by the pandemic, but fraudsters and criminals were also affected, as indicated in a report from the Association of Certified Fraud Examiners.[4] The longer the lockdowns and other restrictions persisted, the more frequent fraudulent and corrupt behaviour became, increasing by almost 80 per cent on average.

By contrast, companies admitted that it had become more difficult to investigate and, in particular, detect misconduct.[5] This poses an especially high risk to companies whose employees have had to endure a work environment fraught with uncertainty, prolonged lockdown and other restrictions, and a sense of urgency in their day-to-day business.

Altogether, this has created a particularly demanding scenario for companies' board members and managing directors, who, on the one hand, had to deal with short-term to medium-term lacks of liquidity, restrictions and supplier shortages and, on the other hand, had to ensure compliance within their companies – all of which form part of their management duties.

Although all those events and risks have been clouding companies' compliance goggles, now is a crucial time for companies to endorse culture. How do you protect your business and eliminate unnecessary risk? And what should be done to prevent various entities from using these times as an opportunity for self-gain?

A representative of a company who is wondering whether its CMS is effective may consider the following questions.

- Is the company's management on all levels committed to compliance, with a zero-tolerance attitude? Would the company's subordinates confirm it if asked anonymously?
- Can the company convincingly explain to local prosecuting authorities, among others, why it has opted for the measures it has implemented and how they could detect a crime?
- Can the employees explain why they follow concrete procedures?
- Are the company's internal procedures adjusted to take into account changes in local laws and circumstances?

4 Association of Certified Fraud Examiners' report 'Fraud in the Wake of COVID-19: Benchmarking Report'.

5 ibid.

Conduct and (online) tone from the top

With the focus during the pandemic and the war on financial resilience, we have often looked at leadership's approach to a company's compliance; however, is the role leadership really the only one that is key?

Indubitably. Commitment by management (on all levels) is the most critical element of a functioning CMS – even more so in times of great uncertainty. Exemplary leadership is a key driver for employee behaviour. Senior and middle management should frequently express their commitment to compliance to help ensure employees understand that compliance remains a priority for the company, as employees will look to their leaders for guidance on how to do business and how to work despite restrictions, as well as for peace of mind.

This requires some clarification. Employees often incorrectly assume that phrases such as 'expressing commitment to compliance' are merely 'empty corporate speak'; however, a leader does not have to be detached from employees. On the contrary, the more the leader detaches himself or herself from his or her subordinates, the less genuine and credible he or she is perceived. There is no reason why a leader cannot express commitment to compliance through, for example, a meme posted in a team WhatsApp chat if appropriate.

CMS: fake versus real

Despite its key role, it still comes as a surprise to many companies that authorities in the CEE region also expect them to have a real CMS in place. A real CMS must be effective and well implemented, with a clearly defined and simple process flow. It must be adapted to the firm's needs and support its business.

By contrast, a 'fake' or superficial CMS exists where risk assessment is only theoretical, where it does not operate as an organic process, does not adapt to the business set-up and where responsibilities and process flow are only superficially defined. This type of 'compliance' is compliance by declaration only, and it is increasingly being sanctioned. Further, tremendous risks and future costs arise for companies, directors and shareholders that do not address fake compliance.

What if non-compliance results in investigations under lockdown?

Compliance is also a business concern, and it is costly if performed badly. Failures in this area are extremely expensive and damaging to reputation. Companies and members of their boards face significant criminal sanctions, fines or bans from participating in

tenders if they fail to investigate non-compliance, as most countries in the CEE region actively prosecute companies for crimes, in particular those pertaining to corruption, money laundering and tax evasion.

Companies' board members must not only implement appropriate procedures to prevent misconduct, but must also investigate any detected misconduct, which often includes formal corporate investigations. If a board member suspects misconduct but does not ensure that it is diligently investigated, then he or she risks liability for breach of fiduciary duties, and the company could hardly claim that it had an effective CMS in place if its board members, managers, etc, do not follow it.

Most jurisdictions in the CEE region either allow companies to release themselves from criminal liability if they prove that they had an effective CMS in place or consider an effective CMS as a mitigating circumstance; thus, the company must react with zero tolerance to any non-compliance and conduct its root cause analysis to be able to effectively improve the CMS.

This may be problematic from a practical point of view. Many activities are still being carried out remotely. Trips and personal meetings have been cancelled and continue to be limited. Consequently, conducting investigations, third-party checks or compliance training is a challenge, and many companies are either withholding their internal compliance meetings and trainings or doing them via videoconferencing. These are vital elements of a CMS.

The same applies for dealing with misconduct. Remote hearings of witnesses or potential suspects takes time and might be more complicated, but companies should not feel discouraged by this, since a great deal of corporate investigations can be done remotely. The trend of shifting investigations into the digital sphere was becoming apparent even before the covid-19 pandemic.

On this basis, companies should apply and strictly abide by the 'document everything' rule so that, at a later date, they are able to prove how certain decisions were taken. Whistle-blower protection is also increasing in importance, with various irregularities and fraud becoming more frequent.

Companies should, therefore, invest further attention in maintaining and developing whistle-blowing platforms to sustain their level of compliance and prepare their business for the aftermath in the event that non-compliance occurs and the authorities return with questions.

For corporate investigations, the situation in the field has changed rapidly. Companies' corporate investigation environments may look very different today from what they looked like one to two years ago and certainly from what they will look

like in the coming years – perhaps because the covid-19 virus has become a common threat or perhaps because its constant mutations will keep human vaccination efforts busy for a few years yet. The war in Ukraine will also bring changes.

For example, the impact of the covid-19 pandemic and the war on interpersonal relationships is enormous. There is little to no direct interaction between co-workers, which is often one of the sources of non-compliance in companies, since colleagues feel safer confiding in their colleagues than in their superiors.

There is also reduced motivation to report issues of concern as the uncertainty and sense of urgency caused by the pandemic or the war might make employees more disorganised, meaning that chaos and non-compliance suddenly becomes more of a standard way of working. Disruption of employees' working routines may also cause problems for investigators, who may struggle to find suspicious working patterns, given that there may not be any reliable routines to follow – even usual work might appear suspicious.

The absence of the usual tools – human resources, time and personal interaction – and logistical barriers to conducting in-person interviews, also makes investigations more detached from employees. Usually, the smallest changes in facial expression and body language can be hugely important sources of information for interviewers, and personal contact affects the interviewee subconsciously in terms of their reaction to the situation, the presence of interviewers and the inescapability of the interview.

With videoconferencing tools, the only sign the interviewer can rely on is the voice of the interviewee. Moreover, a convenient internet outage on the interviewee's side following an unpleasant question can bring an early end to the surprise question. The problem of how video interviews can be seen by interviewees as confidential enough also remains, which results in interviewees being cautious.

On the other hand, remote interviews have several benefits, especially for non-confrontational interviews: interviewees tend to be more open and talkative; elimination of the need to have several people physically in the same place allows for a larger number of interviews to be held within a shorter time frame, which increases efficiency; and the possibility of screen sharing and simultaneous discussion on the contents of certain documents by participants appears to have been very useful in practice.

Finally, having limited access to potentially relevant data means that existing IT infrastructures must provide complete data sets for investigations. Companies that are not yet using clouds should find a dependable solution for collecting data on the work of remote employees.

Such data might not be available owing to privacy concerns; therefore, companies should strive to have in place, or swiftly adopt, the internal policies necessary to govern working conditions during the pandemic and the war, and should inform employees about any compliance audits that may include their personal data.

In some CEE countries, companies are completely prohibited from reviewing data relating to employees who have not been informed beforehand that their data may be reviewed in the event of non-compliance. In others, the review must be very carefully balanced against employees' privacy interests.

An opportunity to improve processes

If the best time to prepare for the crisis was before it happened, the second-best time is now. Crises and urgency help companies to focus. Focus is particularly important when it comes to setting up compliance measures as it enables companies – driven by a sense of urgency – to select only the truly important measures and omit the less important ones.

In theory, this is a no-brainer. CMSs must be simple, clear and easily understandable to employees. This would exclude complex and lengthy processes in which important measures are often diluted by unimportant ones, which often results in less focus but greater obligation. This, in turn, feeds the sense of chaos felt by the average employee who, in the end, may choose simply to ignore it.

So what should be done with existing policies and procedures? Companies' CMSs are generally designed to function under 'normal' operating conditions. A CMS that mitigated risks effectively before may have now become ineffective or even too restrictive, obstructing the normal operation of day-to-day tasks. Other measures may be ineffective and may give companies a false sense of security.

It is, therefore, essential for companies to conduct new risk assessments to understand the areas where they may have new exposures or gaps. Existing risks may need to be reprioritised. One highly recommended solution is the implementation of a graded CMS that is designed to work under various conditions. With this solution, the 'covid-19 mode' (including post-covid-19) could be triggered if the situation deteriorates, with some measures being alleviated and other more stringent measures being established, and vice versa if the situation improves.

Regarding the current war in Ukraine, it is likely that the changes brought to CMSs during the covid-19 pandemic will require fewer adjustments than those pre-pandemic. There are also likely to be war-related effects and changes from a compliance perspective.

At the same time, both with regard to the pandemic and the migration of companies and employees from war zones, the digital world removes the geographical obstacles to business, compliance and corporate investigations, greatly enhancing their efficiency; however, this is a double-edged sword. CEE countries regulate many things differently (privacy laws, employee interviews, data-gathering and reviewing, etc), and the regulations have geographical obstacles.

Companies should have local jurisdictional obstacles in mind when implementing or unifying regional measures. There have been several occasions where a local company had no local internal policies but had merely adopted other companies' European, US or other foreign policies, which were inadequate locally.

Corporate investigations should not be exempt from this process. The trend in digitalisation and the shifting of companies' employees, documentation and activities online (where possible) will continue regardless of the covid-19 pandemic or the war, which are merely accelerating change. Companies have been handed an opportunity to understand new obstacles to their investigative activities, revisit policies, re-establish priorities and develop a better understanding of their IT infrastructure and employees.

Zero-based redesign of the CMS

Corporate criminal liability being implemented almost CEE-wide, together with the push from international and European organisations to investigate and prosecute corruption, including the European Public Prosecution Office, has resulted in FCPA-like investigations, which are more common and professional.

The best way to significantly improve CMSs and processes – in particular for larger companies – is to apply a zero-based redesign.

For most people (sometimes also the ones tasked with maintaining or creating a CMS), the decision to omit or delete something and to focus on selected key areas is notoriously difficult. The fear of omitting some measures, even though in practice they pose no benefit or do not mitigate any risk, may be paralysing. Minor measures have been stacked on top of one another in old CMSs, resulting in an overcomplicated and stiff set of procedures and rules.

Typically, compliance measures are not monitored for effectiveness over the long term. The worst-case scenario is that, despite employees changing as the companies grow, measures continue to be applied just because they have been applied since time immemorial – even though new compliance employees may have no idea why the measures were set in the first place, and there is no original risk analysis nor other

documentation. In that scenario, the companies would be functioning with a set of old, ineffective and redundant measures based on pre-digital risk assessment that should no longer be relied upon.

If an event of non-compliance occurs and local or international prosecuting authorities open an investigation, they will assess the company's CMS.[6] Companies must shine and show that their CMS is effective and that the criminal activity was possible only because of its sophistication and its bypassing of the CMS. The worst-case scenario tends to be that the company cannot show either of those points.

6 This assessment is becoming similar to the US Department of Justice's 'Evaluation of Corporate Compliance Programs'.

BOGDAN BIBICU
Wolf Theiss

Bogdan Bibicu is a member of the firm-wide investigations, crisis response and compliance practice at Wolf Theiss and he coordinates the practice in Romania. He specialises in corporate investigations, compliance, corporate criminal liability/white-collar crime, asset recovery and related matters.

Prior to joining Wolf Theiss, Bogdan established and built up the local and firm-wide compliance, risk and sensitive investigations practice at another regional law firm. Bogdan has gained extensive experience in various sectors, particularly life sciences, infrastructure, IT/TMT, professional services, engineering, transport and the public sector, where he advised clients on locally and internationally triggered issues and investigations.

Bogdan has also led a number of internal investigations in CEE/SEE and advised on various compliance issues, including setting up various compliance programmes. His expertise is complemented by a wealth of experience in the areas of finance, restructuring and insolvency, projects, TMT, life sciences and pharmaceuticals.

As of 2022, he serves as officer of the Anti-Corruption Committee of the International Bar Association. Bogdan has also published extensively and is a frequent speaker at compliance and anti-corruption events.

JITKA LOGESOVÁ
Wolf Theiss

Jitka Logesová heads the regional investigations, crisis response and compliance practice at Wolf Theiss and specialises in corporate investigations, compliance, corporate criminal liability/white-collar crime and asset recovery.

Before joining Wolf Theiss, Jitka established and built up the firm-wide compliance, risk and sensitive investigations practice at another regional law firm. She was also tasked by the Czech Prosecutor General's Office to help draft the methodology for state prosecutors to evaluate corporate compliance management systems and to educate the Czech state prosecutors in this respect.

Jitka has a breadth of experience in various sectors, where she has advised clients on FCPA-triggered issues and investigations, led a number of internal corporate investigations in Central and Eastern Europe and advised on various compliance issues, including setting up anti-corruption and compliance programmes. She has led multiple pre-acquisition anti-bribery and anti-corruption due diligence processes.

Jitka is the immediate past chair of the IBA's Anti-Corruption Committee and a current member of the advisory board of the IBA's Anti-Corruption Committee. Besides her legal qualifications, she is a certified auditor for ISO 19600 (compliance management systems) and ISO 37001 (anti-bribery management systems). She has also published extensively and is a frequent speaker at compliance and anti-corruption conferences.

JAROMÍR PUMR
Wolf Theiss

Jaromír Pumr specialises in compliance and corporate investigations. His work focuses on corporate criminal liability issues in the Czech Republic, as well as anti-bribery and fraud-related advisory. He regularly assists clients in revising and creating compliance management systems to protect their businesses and minimise potential risks.

Before joining Wolf Theiss, Jaromír gained experience as a government lawyer at the Law and Administration Department of the Czech Ministry of Education. He also worked as a legal trainee at two local law firms, specialising in dispute resolution law.

Wolf Theiss

Wolf Theiss is one of the leading European law firms in Central, Eastern and South-Eastern Europe with a focus on international business law. With 340 lawyers in 13 countries, over 80 per cent of the firm's work involves cross-border representation of international clients. Combining expertise in law and business, Wolf Theiss develops innovative solutions that integrate legal, financial and business know-how.

Pobřežní 12
186 00 Prague 8
Czech Republic
Tel: +420 234 765 111
www.wolftheiss.com

Bogdan Bibicu
bogdan.bibicu@wolftheiss.com

Jitka Logesová
jitka.logesova@wolftheiss.com

Jaromír Pumr
jaromir.pumr@wolftheiss.com

Key Issues on Compliance Programmes and their Enforcement in Russia

Paul Melling, Roman Butenko and Oleg Tkachenko
Baker McKenzie

IN SUMMARY

In recent years, Russia has joined the mainstream in terms of its legislative attack on corruption and bribery in the business sector and in its efforts to both educate its business community on best practices when it comes to anti-corruption and oversee and enforce anti-corruption measures. Without minimising the scale of the problem that Russia faces in achieving those objectives, this article provides an overview of recent anti-bribery and corruption legislative measures and the guidance provided to the Russian business community with regard to those measures and their enforcement.

DISCUSSION POINTS

- Recent anti-corruption legislation provides for corporate as well as individual liability for bribery in both the public and private sector
- Extensive official guidance from the Ministry of Labour on how best to build a compliance infrastructure within an organisation and how best to monitor its effectiveness
- Materials posted online by the enforcement authorities support the task of providing compliance training to both employees and those of third-party service providers
- Obstacles to effective and efficient internal investigations, including strict personal data protection legislation being rigidly applied and limitations on attorney–client privilege
- New opportunities for self-reporting but benefits of self-reporting still open to question

REFERENCED IN THIS ARTICLE

- Law on Combating Corruption
- Law on Advocates' Activities and the Advocates' Community

Unprecedented official guidance from regulators across the globe on corporate compliance programmes has been released in recent years. The guidance has ranged from the Criminal Division of the US Department of Justice's Evaluation of Corporate Compliance Programs released in early 2019 and the French Compliance Function Guide, to the updated guidance on Evaluating Compliance Programmes published in the United Kingdom in January 2020.

Following several large cases involving cooperation between the National Financial Prosecutor's Office, the French Anti-Corruption Agency and the UK Serious Fraud Office, the regulators in the United Kingdom (the 2019 Corporate Co-operation Guidance) and France (the Guidelines on the Implementation of the Convention Judicial Public Interest Agreement) issued helpful guides on cooperation with the authorities, which set out regulators' expectations on data retention and investigation efforts.

Russian authorities have also been busy providing practitioners with insight into the government's expectations for anti-corruption compliance programmes. For the most part, the available guidance on building a compliance programme is consistent with international precedent, although there is still little insight specifically into the conduct of internal investigations and ensuring the possibility of retaining and furnishing evidence, including e-data. What can be said specifically is that, when rolling out a compliance programme in Russia, appropriate provisions in employment contracts and internal HR procedures are of paramount importance.

With that in mind, the Ministry of Labour and Social Security (the Ministry of Labour, the employment regulator) and the standards communicated by it play a key role in the compliance process.

Legislation

Russia introduced an explicit requirement for companies to implement compliance measures in 2012.[1] The law sets out a basic list of measures that serve as an example of the minimum a company should consider implementing to comply with the requirement. The list is non-exhaustive and includes:

- introducing a designated anti-corruption function;
- cooperating with the authorities;
- rolling out policies and procedures to ensure a good-faith operation;

1 Federal Law No. 273-FZ of 25 December 2008 'On Combating Corruption', article 13.3 introduced 3 December 2012.

- issuing a code of ethics and business conduct;
- preventing and resolving conflicts of interest; and
- preventing unofficial reporting and the use of forged documents.

There are no specific standards set by law, even for those measures.

There is also no liability specified for failure to comply with those requirements: the Prosecutor's Office has been making modest efforts to enforce them by issuing written binding orders to comply with the requirements following an inspection. Non-compliance with those orders may entail serious consequences, including potential criminal liability for individual members of management who were responsible yet failed to act.

Having a set of compliance measures is intended to have a tangible effect on a company's liability for corruption. Companies can be held liable under the Code of Administrative Offences for undue payments made on their behalf or in their interests[2] and for the illegal employment of former government and municipal officials,[3] unless they have taken all possible measures to prevent the offence (corporate guilt).[4]

Enforcement practice is not consistent: although in some cases companies were able to successfully plead that their anti-corruption compliance measures were sufficient, in a large number of cases the courts have hardly (if at all) conducted any analysis of the company's measures and whether they could serve as a condition for releasing the company from liability.

Elements of compliance: Ministry of Labour practical guidance

The Ministry of Labour is the authority responsible for the 'development and implementation and advisory/methodological support of measures aimed at preventing corruption in organisations, monitoring the implementation of those measures, and methodological support of such measures'.[5]

2 Article 19.28 of the Code of Administrative Offences. Only individuals can be penalised for criminal offences in Russia; companies are liable for the 'administrative offence' of corrupt payments, a concept similar to the crime of corporate corruption.

3 Article 19.29 of the Code of Administrative Offences.

4 Article 2.1 of the Code of Administrative Offences.

5 Decree No. 610 of the Government of 19 June 2012 (as amended) 'On the Approval of the Regulations on the Ministry of Labour and Social Security of the Russian Federation'.

In this capacity, the Ministry of Labour has issued practical guidelines and recommendations concerning measures to prevent corruption in Russia, and it has been very active in fulfilling this function. Since 2014, it has issued a large number of guidelines and recommendations. We will review the most significant of these below.

State organisations and state companies in Russia, for the most part, roll out their anti-corruption compliance programmes following those guidelines and recommendations, and many privately held companies also rely on them. Although the documents issued by the Ministry of Labour are non-binding recommendations, they serve as benchmarks for the Prosecutor's Office and courts.

The guidelines and the early recommendations were issued in an environment in which anti-corruption compliance was still very new in Russia and, thus, contain a considerable amount of tutorial material on overseas and international anti-corruption regulations, best practice summaries and sample documents.

The guidelines were issued in Russian, and we are not aware of any reliable translation.

Anti-corruption compliance system

The Guidelines for the Development and Adoption by Organisations of Measures to Prevent and Combat Corruption[6] were central to the first set of guides passed by the Ministry of Labour in early 2015. It included the Ministry's insight into what reasonable compliance measures should look like. The guide was last updated in 2018.

In October 2019, the Ministry issued another set of guidelines called Measures to Prevent Corruption in Organisations,[7] which largely reiterates the same provisions but is more detailed and better organised. In line with globally evolving best practices, the more recent recommendations have more of a focus on anti-corruption risk assessment and third-party risk management.

According to the recommendations, the minimum set of compliance policies for a company includes an anti-corruption policy, a code of ethics and a code of business conduct. Other important areas to be covered by a company's normative acts are anti-corruption risk assessment, conflicts of interest, communication and training, internal monitoring and control, and management of third parties (eg, due diligence review, avoiding conflicts of interest and anti-corruption clauses).

6 https://rosmintrud.ru/ministry/programms/anticorruption/015/0.

7 https://rosmintrud.ru/uploads/magic/ru-RU/Ministry-0-106-src-1568817692.8748.pdf.

The principles that, according to the Ministry, the anti-corruption policies of a company should rest on do not come as a surprise to experienced practitioners. They are:

- tone from the top;
- communication of anti-corruption regulations to employees and their involvement in anti-corruption procedures;
- effective compliance;
- adequate assessment of risks;
- communication of expected compliance standards to business partners;
- liability and inevitable punishment for employees irrespective of their position; and
- regular internal monitoring and control.

The guidelines describe what an anti-corruption programme might look like, offer a sample set of measures and outline the process for the introduction and renewal of compliance programmes.

Organising a compliance function is an area in which management enjoys broad discretion. Companies are offered a lot of freedom on how they want to structure their compliance function and what department will be responsible for compliance. Importantly, the compliance unit must have a direct reporting line to top management (but the document is silent on reporting thereafter), be sufficiently staffed and be given the resources and powers to exercise its functions.

The guidelines, in their first edition in 2015, introduced the requirement for companies to conduct anti-corruption compliance risk assessments. They broadly outlined procedures for risk assessment and associated record-keeping. In 2019, risk assessment procedures were addressed specifically by the Ministry of Labour in a special set of recommendations.

Dealing with conflicts of interest and enforcing the relevant policies and procedures is central to effective compliance. The Ministry devotes a large part of the document to explaining the general and more industry-specific rules (eg, detailing the risks for the financial sector and medical and pharmaceutical companies).

The expected standard of cooperation with the authorities includes a number of commitments, including:

- reporting corruption;
- non-retaliation against reporters (Russian legislation on this is, however, pending);
- cooperation with investigators and inspectors; and
- retention of evidence.

Companies are recommended to participate in nationwide anti-corruption initiatives, such as the Anti-Corruption Charter of Russian Business.[8]

Anti-corruption risk assessment guidelines

In September 2019, the Ministry of Labour released Recommendations on the Procedure for Assessing Corruption Risks in an Organisation.[9] The 25-page document is essentially a detailed guide to what anti-corruption risk assessments should be. It also encloses sample documents introduced by companies in Russia, such as a risk assessment plan, a risk modelling report and a comprehensive risks map.

In 2017, the Ministry had already taken steps to issue recommendations for anti-corruption risk assessments, but the 2017 guide only applied to state authorities and state corporations or companies.[10] The new set of recommendations is offered to all entities.

When working on the 2019 risk assessment guide, the Ministry apparently conducted extensive research into international best practice and widely accepted standards of anti-corruption risk assessment.

In our view, the document provides very good guidance, although, in our practice of advising clients in Russia on compliance risk assessment, we seldom come across procedures and records anywhere near so detailed and sophisticated.

The guidelines are organised as a step-by-step procedure for the identification, analysis and ranking of corruption risks. They consistently promote the idea of adequacy of risk assessment procedures for the specific company into which they are to be introduced, for example, based on its size, industry sector and available resources.

The basic recommendation is to start with a calendar plan, identify the priority areas and then progressively roll out risk management procedures to all other aspects of the company's activities. This is a very reasonable recommendation, and clients could benefit from taking it on board. Instead of waiting for the right moment to conduct a comprehensive risk assessment of the entire business, it makes sense to prioritise and start with the high-risk areas.

In identifying high-risk areas, companies are predictably invited to follow value-based and risk-based approaches. Government-facing functions are a priority, including sales via state procurement, obtaining licences, permits and approvals, and

8 http://against-corruption.ru (last accessed: 14 April 2022).

9 https://rosmintrud.ru/uploads/magic/ru-RU/Ministry-0-106-src-1568817604.7941.pdf.

10 https://rosmintrud.ru/ministry/programms/anticorruption/9/8.

dealings with state officials in the course of inspections. Examples of other high-risk areas listed by the Ministry include procurement for company needs, real estate transactions, disposing of property including non-core assets, budgetary functions (providing loans, marketing and sponsorship), use of intermediaries and remuneration or bonus schemes for employees.

Companies are reminded that compliance risks can be created not only by their own employees but also by third parties (agents, consultants and distributors, among others).

When assessing risks, companies are expressly advised to take into account their exposure to the laws of other countries where they (or their business partners) operate, including the US Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act.

The standard set by the Ministry for risk assessment procedures includes collection of data through document review and interviews with key employees, risk modelling, identification of existing risks and controls and their owners, risk ranking, gap analysis and identification of remedial risk mitigation actions.

Employees' obligations and motivation

In October 2019, the Ministry of Labour published its Memorandum on Employee Duties and Motivation in Organisations.[11]

The Ministry explained that the obligation to comply with anti-corruption policies and procedures should be made part of the employment contract and that disciplinary (employment law) sanctions should be consistently applied to employees who fail to meet those obligations.

In addition to the inevitable sanctions for those in breach of their employment contracts, companies are encouraged to introduce monetary and non-monetary benefits as motivation for compliance on the part of their employees. Companies should not discourage employee compliance by setting key performance indicators that lead employees to prioritise performance over compliance.

As everyone with experience in this market is well aware, it is very difficult to sanction employees and especially to terminate their contracts for corruption-related offences in the absence of a valid court verdict against the non-compliant employees. It remains to be seen if enforcement practice will move in the direction of giving companies more opportunity to sanction rogue employees.

11 https://rosmintrud.ru/uploads/magic/ru-RU/Ministry-0-106-src-1568817742.8173.pdf.

In recent years, our firm has won several cases in Russia for clients arising from the termination of the contracts of employees who, according to internal investigations, had failed to comply with internal compliance policies and procedures. Nonetheless, the dominant practice for parting company with the non-compliant employee remains the mutually agreed separation agreement, often coupled with a monetary sum paid to the employee.

Compliance function structure

The Ministry of Labour updated its model job description for the compliance role in 2018.[12] Formally, the guidelines apply to state corporations and state-owned entities; however, private businesses can benefit from this example.

The document sets a ratio of one to 100 as a recommendation for the size of the compliance unit relative to the overall number of employees. In our experience, this is a very generous ratio that is seldom met in the headcount of compliance units in private clients.

Internal investigations remain a relatively unregulated area in Russia. The compliance function guidelines explain, however, that compliance officers should have a right to conduct internal checks, including interviewing employees, subject to this function being included within the scope of their functions by internal regulations.

Prosecutor's Office guidance

The Prosecutor's Office (together with its territorial subdivisions) is the main driver of enforcement practice for corporate corruption offences, as it is the authority in Russia that investigates corporate corruption cases under article 19.28 of the Code of Administrative Offences.

Prosecutors also perform the function of overseeing compliance with anti-corruption laws in accordance with the international treaty obligations of Russia. Designated anti-corruption compliance departments have been established at all levels of the Prosecutor's Office. As part of this function, they make enquiries into the existence of corporate compliance programmes. Prosecutors are frequent speakers at compliance conferences and roundtables.

12 https://rosmintrud.ru/ministry/programms/anticorruption/015/1.

The anti-corruption compliance department of the Prosecutor's Office on its designated website[13] publishes a wide range of educational materials that compliance managers may find helpful in their work, especially if they have limited resources. Local companies with international best practice support from global headquarters can also benefit from those materials. Particularly worthy of mention are the Prosecutor's memoranda on Corporate Liability for Corruption and Gifts to Public Officials.

The Prosecutor's website even hosts videos with role-played high-risk situations, which fit very well into internal compliance training programmes.

Internal investigations

The ability to conduct effectively internal investigations into corruption and related allegations is a hugely important element of an effective compliance programme; however, this aspect of the work of compliance managers and counsel remains a blank area in the Russian regulatory framework. There is almost no official guidance or reliable enforcement practice.

Practitioners often have to rely on their own interpretation of local laws and follow international best practice. This makes internal procedures (eg, investigation policies, rules on the use of corporate devices and IT systems and use of the company's property for private purposes) key to the process, and companies should properly issue them as local normative acts.

The most problematic aspects of internal investigations include the treatment of personal data, correspondence and private information collected during the investigation, protection of attorney–client communications and work products and reporting internal findings to the authorities.

Personal data, correspondence and private information

The Law on the Protection of Personal Data and legislative requirements for the localisation of individuals' data in Russia have set the bar very high in protecting privacy in any internal investigation conducted in Russia.

In the absence of any official clarifications or court practice, the safest option to comply with the data privacy requirements is to seek written consent from all those being interviewed to any transfer of that person's personal data (even to associated companies in the same corporate group). Two options are possible:

13 https://epp.genproc.gov.ru/ru/web/gprf/activity/combating-corruption/combating-corruption-in-proc/met.

- consent can be obtained in advance of any investigation being required but should clearly state the purpose (ie, verification of correspondence to internal company policies and procedures); or
- specific consent can be obtained from the data owners at the beginning of the investigation.

If, for any reason, it is not possible to obtain consent, the investigating entities may invoke other legal grounds for personal data processing that do not require the employees' consent. For example, as the ultimate goal of internal anti-corruption investigations is to eliminate non-compliance with legislation and (probably) local internal policies, the processing of employee data within the investigation can be based on such legal grounds as:

- the necessity to achieve the objectives set out in Russian legislation; or
- the necessity to exercise the rights and legitimate interests of the operator or third parties.

Although this approach seems logical and is based on the law, we are not aware of any positive enforcement practice using this interpretation.

Properly documenting the investigation is essential. Companies should officially initiate the investigation with an order of the general director appointing individual investigators as the authorised representatives of the employer. In this case, the investigators will have access to the employees' data on behalf of the employer even without the written consent of the employees. The investigation must be completed within strict deadlines and end with another order of the general director reporting the findings.

Internal investigations do not usually target information about an employee's private life, but today's working environment makes it impossible to draw a clear division between one's private and professional life, especially for those who work with 24/7 availability. It is, therefore, commonplace for employees to store some pieces of information about their private life (eg, private photos, documents and correspondence) on their corporate devices. This information, if accidentally found, should be ignored and not used in the investigation. Search terms should be carefully formulated to minimise the risk of encountering this information.

There is criminal liability in Russia for the illegal collection or distribution of data about an individual's private life containing a personal or family secret without his or her consent, although a criminal prosecution for truly unintended collection of information on an individual's personal life cannot be justified. An appropriate internal

policy on use of corporate IT solely for business purposes can be helpful in supporting a position that all information found on corporate IT must be business-related or in supporting an argument that by placing such information on corporate IT, the employee has de facto consented to it being accessed.

Protection of attorney–client communications and work product

It is common knowledge that the Russian legal system has a different approach to the concept of legal privilege when compared with common law jurisdictions.

In Russia, irrespective of the area of law, legal advice and representation in court proceedings may be provided by advocates (practitioners who are the members of a Bar) and other legal practitioners persons with few limitations;[14] however, professional secrecy is protected only in relationships between clients and advocates.

Article 9 of the Federal Law on Advocates' Activities and the Advocates' Community defines an advocate's secret very broadly: any information related to the provision by the advocate of legal services to his or her client. The article also provides three types of guarantee against disclosure of this sensitive information:

- prohibition on calling and questioning advocates as witnesses concerning matters known to them in relation to their legal services;
- prohibition on searching advocates' premises, except on the basis of a court order; and
- prohibition on using materials contained in the advocate's file (called a dossier) as evidence for prosecution of the advocate's clients.

The Criminal Procedural Code provides additional guarantees to protect advocates from pressure from the law enforcement authorities. In particular, it establishes a special and complex procedure for initiating criminal cases against advocates. A decision on the initiation of a criminal case against an advocate must be taken by the Regional Head of the Investigative Committee.[15] Mandatory escalation of the matter to this high level is aimed at decreasing the risk that low-level officers put pressure on the advocate by commencing an arbitrary criminal case against him or her.

14 For example, generally, practitioners who are not members of a Bar cannot act as defence attorneys in Russian criminal proceedings.

15 Article 448, sub-clause 1.10 of the Criminal Procedural Code.

In post-Soviet Russia, the Constitutional Court, in a number of cases,[16] stressed that advocates enjoy special protection from search and seizure. Some cases have been escalated to the European Court of Human Rights (ECHR), where legal advisers other than advocates have been seeking similar treatment.

In an important case against Russia (*Kruglov and others v Russia*),[17] the court stated that it would be incompatible with the rule of law to leave without any particular safeguards to the relationship between clients and their legal advisers who, with few limitations, practise, professionally and often independently, in most areas of law, including representation of litigants before the courts.

In this regard, the court found that searches without judicial authorisation of the premises of the applicants in that case, who were practising lawyers but not advocates, had been conducted arbitrarily.[18] The ECHR underlined that practitioners who do not have advocate status should, therefore, enjoy the same safeguards on the protection of privileged documents and information as advocates possess.

It remains to be seen how this ECHR opinion will affect Russian practice. Thus far, Russian law has not been amended. It still provides protection for privileged information only to legal professionals who are advocates. We believe that unless and until privilege protection is introduced as a new law, any documents and information seized from the premises of professionals who are not advocates would be admissible evidence in Russian courts.

Even the participation of advocates in an investigation is not an absolute guarantee against disclosure of their privileged documents. Cases of attorney-client privilege violation by Russian law enforcement authorities are still reported even where advocates are involved.

However, the community of advocates vigorously defends its members and their exclusive rights provided by the law, with cases of violation receiving massive press coverage and having decreased substantially over recent years. All those efforts have had a positive effect on law enforcement practice and have resulted in a more cautious

16 See, for example, Resolution of the Constitutional Court No. 33-P, dated 17 December 2015

17 European Court of Human Rights (ECHR) judgment dated 4 February 2020.

18 In the case in question, the investigating authorities had obtained judicial authorisation for the searches in respect of the advocates, in accordance with the procedure prescribed by law. For example, para 121, 122, 137 of the ECHR judgment *re: Kruglov and others v Russia*, dated 4 February 2020.

approach by the law enforcement authorities towards violating attorney-client privilege. Violations of Russian law concerning attorney-client privilege and involving advocates is now rare.

In view of the above, and taking into account the unpredictable law enforcement environment in Russia, it is not surprising that companies hire advocates to conduct internal investigations.

Self-reporting under Russian law

In 2018, Russian law was updated to include provisions on the voluntary disclosure of corruption offences by companies.[19] (A similar provision of self-reporting agreements violating antitrust law had been part of Russian law since 2017.)[20]

In particular, companies are released from liability for a corporate corruption offence if they contributed to the uncovering of the offence, assisted in the administrative investigation or the uncovering and investigation of the crime, or if they faced extortion. At the same time, Russian law contains no liability for the non-reporting of corruption offences.

The enforcement practice around those new legal provisions remains inconsistent. There have been a number of cases where the courts applied this provision to release companies from liability; however, there have also been cases where courts declined to apply this provision in seemingly similar circumstances. The enforcement authorities have not issued any guidance for evaluation of a company's efforts towards self-reporting and, in their public presentations, have mostly concentrated on the proper timing of self-reporting.

In respect of timing, a decision to release from liability on the grounds of self-reporting can be taken either by the enforcement authorities at an early stage of proceedings under the Code of Administrative Offences or by the courts in the subsequent public proceedings; thus, self-reporting could very easily lead to no benefit at all if the prosecutor declines to release the company from liability and proceeds to bring the case to court.

Clearly, companies should carefully consider the risks related to self-reporting on a case-by-case basis. Among the other factors to be taken into account are the following:

- commencement of a criminal investigation into corruption involving employees of the company or business partners;

19 Article 19.28 of the Administrative Code, note 5.

20 Article 14.32 of the Administrative Code, note 5.

- known facts of self-reporting of a suspected individual in his or her personal capacity;
- disruption to business caused by various investigative measures;
- self-reporting triggers under applicable anti-corruption laws in other jurisdictions; and
- the potential amount of the fine that could imposed for the offence (fines could reach 100 times the amount of a bribe or proposed bribe).

Conclusion

To some, the very notion of comprehensive anti-corruption legislation and compliance practices in Russia may come as a complete surprise, but only if you missed out on the fact that Russia's days as 'the Wild East' are many years behind it.

This is not to say that Russia will likely be making a rapid climb up the Transparency International Corruption Perceptions Index any time soon. What it does mean, however, is that in driving home the message of ethical business practices and the importance of eradicating bribery and other forms of corruption, a multinational corporation no longer has to reference the FCPA or the UK Bribery Act; instead, it can reference the (almost identical) obligations of the business under Russian law and the substantially similar local guidance on meeting those obligations.

PAUL MELLING
Baker McKenzie

Paul Melling is an English solicitor who has spent his entire professional career working in the countries of the former USSR, having opened Baker McKenzie's Moscow office in January 1989. He has been resident and practising law in Moscow for over 30 years. In addition to being the founding partner of Baker McKenzie Moscow, he also opened his firm's Almaty office in 1995. He is the founder and leader of Baker McKenzie's compliance and investigations group in Moscow. He is also honorary legal adviser to the British Ambassador to Russia and a member of the Advisory Council of the Russo–British Chamber of Commerce.

Paul is known particularly for his work with multinational corporations in the life sciences sector (both pharmaceuticals and medical devices). In *Chambers Europe 2020*, he was ranked as an 'Eminent Practitioner' in the life sciences section and, as far back as 2009, he received the Distinguished Service Award from the Association of International Pharmaceutical Manufacturers for his 'Outstanding Contribution to the Development of the Russian Pharmaceuticals Market'.

ROMAN BUTENKO
Baker McKenzie

Roman Butenko is a senior associate in Baker McKenzie's Moscow office and a criminal advocate admitted to the Moscow city bar. He is experienced in the area of anti-bribery compliance and investigations, criminal law and dispute resolution. Roman has a PhD in law and is a visiting lecturer at the Russian Ministry of Economic Development, as well as at a number of leading Russian universities, where he lectures on anti-corruption compliance matters.

Roman has extensive experience in internal investigations and compliance advisory work across various regions and industries, including healthcare, TMT, energy and mining, and others.

Roman spent around one year in the Washington, DC office of Baker McKenzie, where he advised and assisted clients on various anti-bribery compliance matters. He has also gained the unique multicultural experience of advising and representing clients across Central Asian jurisdictions during his over two-year practice in Almaty, Kazakhstan.

OLEG TKACHENKO
Baker McKenzie

Oleg Tkachenko is counsel with the Moscow office of Baker McKenzie and a Russian advocate. He focuses on criminal law and procedure and also specialises in investigations and litigation. He obtained this status and was admitted to the Moscow Region Advocates Chamber in 2004.

Oleg is a former tax police officer. He worked at the Central Office of the Russian Tax Police from 2001 until 2004. His experience includes defence in a wide range of criminal cases and representation of victims, as well as assisting with searches and seizures, interrogations and internal investigations. Oleg was recommended for criminal proceedings and white-collar crime-related issues by *The Legal 500 EMEA 2020*.

Baker McKenzie.

For more than 70 years, Baker McKenzie has been effectively providing global advice for large domestic and multinational clients and for over 30 of those years providing such advice in Russia. The size and global reach of our firm, with its 78 offices in 46 countries, guarantees that know-how is shared among jurisdictions and allows resources from our international network to supplement local office needs. Our lawyers advise clients on criminal and criminal procedure law issues, represent clients and their management before law enforcement authorities and regulators and lead internal investigations in response to allegations of the violations potentially leading to criminal and administrative liability (white-collar crimes). Baker McKenzie was ranked as a leading law firm in Russia for its white-collar crime practice in *The Legal 500 EMEA 2020*.

White Gardens, 10th Floor
9 Lesnaya Street
Moscow 125196
Russia
Tel: +7 495 787 2700
www.bakermckenzie.com

Paul Melling
paul.melling@bakermckenzie.com

Roman Butenko
roman.butenko@bakermckenzie.com

Oleg Tkachenko
oleg.tkachenko@bakermckenzie.com

The Shifting Landscape of Investigations in the GCC

Darren Mullins, Paul Wright, Wendy Robinson and Rae Lawrie
Accuracy

IN SUMMARY

Gulf Cooperation Council (GCC) countries have implemented many monitoring, regulatory and legal initiatives to address the risks of criminal exploitation during the pandemic while dealing with ever-changing technologies and winning the trust of overseas investors. These initiatives have presented many challenges and opportunities for corporate investigators. This article discuss the details of some of the changes and their likely impact on regional investigations.

DISCUSSION POINTS

- Current regulatory and legal landscape in the GCC
- The impact of data privacy laws
- Stricter counterterrorism and anti-money laundering (AML) controls
- The impact of bankruptcy and insolvency laws
- The change in the cybercrime landscape
- The advent of cryptocurrency and the need for investigation

REFERENCED IN THIS ARTICLE

- GCC economic vision
- Data privacy laws
- AML and FATF
- Bankruptcy and insolvency laws
- Cybercrime laws
- Cryptocurrencies
- Crypto investigations

Introduction

The Gulf Cooperation Council (GCC), comprising the Kingdom of Saudi Arabia (KSA), the United Arab Emirates (UAE), Qatar, Bahrain, Oman and Kuwait, has seen strong economic growth over several decades. Most GCC countries are continuing to seek outside investment to support their ambitious development plans (eg, Saudi Vision 2030, Dubai 2040 Urban Master Plan, Abu Dhabi 2030 Economic Vision, Qatar National Vision 2030 and Kuwait Vision 2035).

Although the GCC has managed sustained economic growth, the corporate investigations landscape has struggled for many years to keep up with the demands of companies faced with numerous risks owing to underdeveloped regulatory and legal frameworks in GCC countries. Those who wish to prey on individuals and corporations through fraud, cybercrime and misconduct have exploited the regulatory and legal gaps, and there is also significant regional exposure to sanctions-related issues and money laundering threats from organised crime.

Recognising these risks, GCC governments have worked to adapt both their regulatory and legal frameworks in recent years to make their economies more attractive to outside investors, including by investing heavily in initiatives to counter the threat of crimes and regulatory breaches and to reduce criminal activity. For example, authorities in the GCC have sought to modernise their regulatory regimes through, among other things, enhanced regulatory monitoring and harsher penalties relating to cybersecurity, digital identity, digital currencies, fintech, anti-money laundering (AML), data protection and privacy, and terrorist financing.

These initiatives are in addition to guidance issued in response to the covid-19 pandemic and increased international cooperation on transparency, extradition and money laundering targets. These modernisation efforts, although sometimes slow, have also seen the establishment of new regulators.

Data privacy laws

As of March 2022, five countries in the GCC have enacted new data privacy laws to strictly monitor and control the use of personal data:

- KSA Royal Decree M/19 of 9/2/1443H;[1]
- UAE Federal Decree-Law No. 45 of 2021;[2]

1 Published in the Official Gazette of September 2021.

2 'Overview of UAE's Federal Decree-Law No. (45) of 2021 on Personal Data Protection (PDPL)', *Securiti* (2021).

- Qatar's Data Protection Law No. 13 of 2016;
- Bahrain's Law No. 30 2018;[3]
- Oman's Royal Decree 6/2022;[4] and
- Law No. 5 of 2020 of the Dubai International Finance Centre (DIFC).

The GCC countries join more than 130 jurisdictions with comprehensive privacy laws intended to safeguard individuals against the misuse of their personal data by organisations that receive or use such data. The GCC regulations bring regional laws in line with international standards, and there are strict penalties for the misuse of data or breaches of the law, with fines reaching up to US$800,000 in KSA and two years' imprisonment for the misuse of sensitive data.[5]

These regulations potentially impact global organisations as the territorial scope encompasses any organisation that carries out processing activities about data subjects[6] in the GCC, regardless of where they are established.

In this sense, the regulations are similar to the EU General Data Protection Regulation (GDPR), under which the authorities have issued more than 900 fines since its inception in 2018 across the European Economic Area and the United Kingdom, punishing organisations such as Amazon (US$877 million)[7] and WhatsApp (US$255 million).[8] Properly implemented and enforced, the GCC regulations could be similarly punitive to organisations that fail to prepare and change adequately.

The impact on corporate investigators is twofold: the first impact is when a breach is suspected and needs to be investigated and reported by the organisation. Many of the regulations require a reporting mechanism (typically through a commissioner or a data office). To respond to such a situation, organisations should work closely with their investigators and compliance officers to put in place and implement appropriate policies and procedures.

---

3 Law No. 30 of 2018 with respect to the Personal Data Protection Law.

4 Royal Decree 6/2022 promulgating the Personal Data Protection Law, published in Official Gazette No. 1429.

5 'Global Data Privacy & Security Handbook – Saudi Arabia', Baker McKenzie (23 January 2020).

6 A data subject is a natural person who can be identified directly or indirectly by specific information (personal data).

7 Sam Shead, 'Amazon hit with $887 million fine by European privacy watchdog', CNBC (30 July 2021).

8 Conor Humphries, 'WhatsApp fined a record 225 mln euro by Ireland over privacy', *Reuters* (2 September 2021).

The second impact is how investigators gather and process information to pursue an investigation. Consideration must be given to receiving a data subject's consent to handle the data or confirm that there is a lawful circumstance for its processing. In the context of an investigation that may include gathering and processing personal data, a lawful purpose could comprise any of the following:

- where the data subject has made the personal data public;
- protection of the interests of the data subject;
- being part of a judicial or security procedure; or
- medical purposes or matters of public health.

Terrorism and AML

The global community has made AML and combating the financing of terrorism (CFT) a priority. These efforts aim to guard the integrity of the international financial system, cut off the assets accessible to terrorists and make it harder for those engaged in wrongdoing to profit from their felonious activities.

Money laundering is secondary to a primary crime, such as corruption, drug trafficking, human trafficking, fraud and cybercrime. The original crime is called a predicate offence, and it is how bad actors acquire 'dirty money'. Stopping money laundering can help stop primary offences and further help prevent the diversion of money away from financially productive uses. These diversions can have damaging impacts on businesses and the financial sector.[9]

The Financial Action Task Force (FATF) on money laundering, a 39-member intergovernmental body established by the 1989 G7 Summit in Paris,[10] has primary responsibility for developing the global standards for AML and CFT (AML/CFT). It works in close cooperation with other key international organisations, including the IMF.

Certain GCC and neighbouring countries have sought the assistance of the FATF in assessing their AML regulatory regimes. Saudi Arabia, the UAE, Bahrain, Egypt and Jordan have completed the fourth round of mutual evaluations by the FATF, with

9 The negative consequences of these financial wrongdoings have resulted in the International Monetary Fund (IMF) being very active for over ten years in the anti-money laundering (AML) and combating the financing of terrorism (CFT) arenas. The IMF's unique blend of global membership, surveillance capabilities and financial sector expertise makes it a central and crucial element of international AML and CFT efforts.

10 FATF, 'History of the FATF'.

Qatar currently going through the process. As of March 2022, the UAE, Jordan and Yemen are listed in the FATF's grey list, meaning they are listed as high-risk countries, which can negatively impact investments.[11]

The UAE is taking steps to shed its reputation as a financial crime hotspot. In 2021, the UAE's central bank fined 11 banks a total of US$12.5 million for having inadequate AML and sanctions controls at the end of 2019.[12] It has also stepped up its AML/CFT enforcement efforts, with new extradition deals planned with several countries and several cross-border training operations.

Further, changes in the UAE's legislation and the development of enforcement guidelines have advanced money laundering investigations and prosecutions.[13] For instance, the UAE has updated key legal instruments, such as Federal Decree-Law No. 20 of 2018 on AML/CFT, which has been further enhanced and amended through Federal Decree No. 26 of 2021.

The UAE's grey list placement initially led to increased investigations prior to the covid-19 pandemic, particularly regarding shareholder disputes as companies were more sensitive to the risk and therefore conducted more internal investigations. Some of this increase in investigations also resulted from, for example, the change in company law in the UAE[14] and regulatory investigations in the pharmaceutical industry.

However, inquiries and reviews stalled as companies looked to control costs while having to rapidly revise policies and procedures as remote working became the norm. There has not yet been a spike in the number of investigations in the wake of the covid-19 pandemic; however, with global indicators showing a massive increase in fraud and corruption,[15] it is highly likely that there will be an increase in investigations (along the lines of the exponential growth in investigations that occurred in the aftermath of the financial crisis in 2008).

11 FATF, 'Jurisdictions under Increased Monitoring – March 2022'.

12 John Basquill, 'UAE threatens anti-money laundering crackdown as 11 banks fined', *Global Trade Review* (3 February 2021).

13 Rola Alghoul, 'UAE releases 4th issue of Al Manara: Anti-Financial Crime Newsletter of UAE Emirates News Agency', *Emirates News Agency* (15 February 2022).

14 United Arab Emirates government portal, 'Full foreign ownership of commercial companies'.

15 'Global Fraud Trends: Device Insights Highlight Increased Threats Since Onset of Pandemic', *TransUnion* (22 March 2021).

Bankruptcy and insolvency regulations

GCC countries have also sought to become a more attractive home for investment by creating more modern, recognisable insolvency regimes that contain modern restructuring tools for businesses facing distress. The KSA, Bahrain, Oman, Kuwait and the UAE have either brought in new laws or updated existing laws to make them more investor friendly and, in some cases, to decriminalise certain aspects related to personal insolvency. The World Bank sees these creditor rights and insolvency systems as being of key importance in providing investor confidence in these countries.[16]

Given these updated insolvency laws, liquidation is no longer the last resort for companies in those jurisdictions. As a result, companies are now conducting more internal investigations to understand if fraud or management errors may be leading the companies to insolvency or bankruptcy rather than just bad business practices or market pressure; in the past, companies and individuals ran the risk of imprisonment for non-payment of debts, which led to companies trying to delay liquidation.

As an example, one of the first companies to utilise the new KSA bankruptcy law in the past year was Ahmad Hamad Al Gosaibi & Brothers (AHAB) after a global dispute with Maan Al-Sanea and the Saad Group. Prior to the new law, AHAB had few options to restructure its debt other than to go into liquidation. This would likely have led to the break-up of the family partnership businesses (most of which were operating at a profit), the loss of all the partners' personal assets and possible imprisonment for the partners.

In 2021, the KSA court ratified AHAB's efforts to restructure US$7.5 billion of obligations with over 100 local and international financial institutions, thus bringing an end to a prolonged investigation and litigation that extended for more than 12 years.[17]

The applicable recent regulations are:

- the UAE Bankruptcy Law No. 9 of 2016, which was later amended by Law No. 21 of 2020;
- the KSA Bankruptcy Law, introduced in 2018;
- the Bahrain Reorganisation and Bankruptcy Law No. 22/2018;
- Kuwait's Law No 71. Of 2020; and
- Oman's Royal Decree 53/2019.

16 'Principles for Effective Insolvency and Creditor/Debtor Regimes, 2021 Edition', World Bank.

17 Matthew Martin, 'Saudi Conglomerate's $7.5 Billion Default Is Finally Settled', *Bloomberg* (15 September 2021).

Cybercrime laws and regulations

The global cost of cybercrime is expected to hit US$10 trillion in 2025, according to a 2021 cyberwarfare report by Cybersecurity Ventures.[18] These figures showcase the enormity of the threat of cyber-attacks and breaches.

At the regulatory level, the most potent deterrents for this type of crime are strict regulations and penalties for using technology to commit or facilitate a crime, and several GCC countries have recently adopted laws in this space. For instance, the UAE's latest Cybercrime Law[19] addresses hacking, fake news, impersonation, internet bots and cryptocurrency and provides a framework for harsher penalties for breaches of the law.

The KSA's Anti-Cybercrime Law of 2007,[20] the Qatar Cybercrime Prevention Law,[21] the Oman Cybercrime Law[22] and Kuwait's Combating Information Technology Crimes[23] all address cybercrime to varying degrees, although they require updating to be in line with the latest technologies used to undertake cybercrime, such as the misuse of cryptocurrencies and non-fungible tokens.

As of April 2022, the DIFC and the Abu Dhabi Global Market have announced plans for the regulation of crypto assets and have already established that crypto exchanges will be regulated under these authorities going forward.[24]

With these new laws and regulations in place, criminals are moving to new methods of making profit. Many illegal gains are now obtained or laundered through deregulated cryptocurrencies. Cryptocurrencies pose unique challenges to investigators charged with identifying, tracing or seizing illicitly gained funds and assets.

---

18 Steve Morgan, 'Cybercrime To Cost The World $10.5 Trillion Annually By 2025', *Cybercrime Magazine* (13 November 2020).

19 'Joint statement on the UAE's adoption of Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrime', *ADHRB* (24 January 2022).

20 Kingdom of Saudi Arabia Bureau of Experts at the Council of Ministers, Anti-Cybercrime Law, Royal Decree No. M/17 of 26 March 2007.

21 Nabeela, 'Cyber crimes in Qatar: The law and how to report them', *ilovequatar.net* (29 April 2020).

22 Alice Gravenor, 'Oman: Latest developments in data protection and cybersecurity', *DataGuidance* (September 2020).

23 Council of Europe, 'Kuwait, Cybercrime Legislation' (15 April 2020).

24 Felicity Glover, 'DFSA publishes regulatory framework to oversee cryptocurrencies', *The National* (10 March 2022).

Cryptocurrency

Blockchain-based cryptocurrencies allow individuals to engage in peer-to-peer financial transactions or enter into contracts as decentralised platforms. In either case, there is no need for trusted third-party intermediaries.

A cryptocurrency is generally defined as digital tokens or 'coins' on a distributed, and decentralised ledger called a blockchain. Since the launch of bitcoin in 2008, the types of cryptocurrencies have expanded dramatically.[25] Bitcoin continues to lead the pack of cryptocurrencies in terms of market capitalisation, user base and popularity.

Other virtual currencies, such as Ethereum, are helping to create decentralised financial (DeFi) systems. Some 'altcoins' have features that bitcoin does not, such as handling more transactions per second or using different algorithms (eg, proof of stake).[26]

Several cryptocurrencies have built-in privacy features or preferences that users can use for more private online commerce.

Troublesome trends

The two key ways in which criminals obtain cryptocurrency are:

- stealing the funds directly; or
- using a scam to trick individuals and organisations into parting with it.

In 2021, crypto criminals stole a record US$3.2 billion-worth of cryptocurrency, according to Chainalysis. That is a fivefold increase on the year before.

Scams continue to surpass outright theft, enabling criminals to swindle US$7.8 billion-worth of cryptocurrency from victims.[27]

25 Taylor Locke, 'Bitcoin launched 13 years ago this month — here are 8 milestones from the past year', *CNBC Make It* (3 January 2022).

26 A proof of stake consensus algorithm is a set of rules governing a blockchain network and the creation of its native coin.

27 'Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity', *Chainalysis* (6 January 2022).

There are several different theft-related trends that investigators should be concerned about. First, most scam-related thefts are 'rug pull' scams. Rug pull scams are a relatively new modus operandi in which the crypto criminals 'pump' the value of their coins before vanishing with the coffers, leaving their investors with zero-valued assets.[28] These scams are not always illegal, but they are always unethical.[29]

Another new scam targets people online, with victims persuaded to invest in fake cryptocurrency schemes. The scam often combines romance fraud with crypto cons, as victims are promised a 'happily ever after' and big crypto gains. The cybercriminals operating this long con spend months gaining online daters' trust, using romance and the lure of fast crypto returns to trick victims out of their savings. Once the crypto criminal has drained their victim, or when the victim realises they cannot withdraw any of the funds they believe they have invested in the scheme, the perpetrator will disappear.

These facts make crypto crime a fast-growing business, giving criminals an incentive to invest time and money to make money. The rise of the crypto economy and DeFi, coupled with record cryptocurrency prices in 2021,[30] has provided criminals with profitable openings. Former US federal prosecutor Jessie Liu emphasised this point when she stated earlier this year: 'The DOJ has seen cryptocurrency used to "professionalize" cybercrime because bad actors are using digital assets to purchase illicit services such as computer hackers or ransomware software.'[31]

Prosecutors, investigators and regulators are right to be concerned about these current trends and the impending ability for criminals to use cryptocurrency as part of their arsenal of tools to commit crimes. Buyers risk losing all their money invested in crypto assets and could fall prey to fraud. The European Union's securities, banking and insurance watchdogs said: 'Consumers face the very real possibility of losing all their invested money if they buy these assets.'[32]

---

28 US Attorney's Office press release, 'Two Defendants Charged In Non-Fungible Token ("NFT") Fraud And Money Laundering Scheme' (24 March 2022).

29 'Crypto rug pulls: What is a rug pull in crypto and 6 ways to spot it', *Crypto News* (6 February 2022),

30 Niccolo Conte, 'This is how the top cryptocurrencies performed in 2021', *World Economic Forum* (26 January 2022).

31 Sam Fry, 'Former money laundering prosecutors predict aggressive US crypto seizures', *Global Investigations Review* (3 March 2022).

32 'Be ready to lose all your money in crypto, EU regulators warn', *Reuters* (18 March 2022).

Regulators are increasingly worried that more consumers are buying different crypto assets (17,000 by one count),[33] including bitcoin and ether, which account for 60 per cent of the market, without being fully aware of the risks. They are also working hard to develop crypto asset regulations that will help make this type of investment safer for consumers. This initiative could herald more widespread adoption once markets in multiple jurisdictions recognise that it is possible to regulate crypto asset service providers and protect crypto asset investors.

Current status

In February 2022, the US Department of Justice (DOJ) declared a milestone seizure of 94,000 bitcoin estimated to be worth over US$3.6 billion – the DOJ's largest-ever haul of cryptocurrency and the largest single financial seizure in the department's history.[34]

Will there be more seizures of this magnitude? Crypto firms in times of financial adversity may receive requests to liquidate large sums of virtual currency as individuals and companies seek a safe (government-backed) refuge for their fortunes. Some exchange clients use cryptocurrency to invest in real estate, while others want businesses in countries such as the UAE to turn their virtual money into hard currency and store it away from harm's way.

Dubai, the GCC's financial and business centre and a growing crypto hub, has long been a magnet for the rich. This has also resulted in it being a destination for illicit money. As mentioned, this has resulted in the financial crime and money laundering watchdog, the FATF, putting the UAE on its grey list in March 2022 for increased monitoring.[35] The UAE responded by asserting its commitment to strengthening AML/CFT efforts.[36]

33 Megan DeMatteo, 'There Are Thousands of Different Altcoins. Here's Why Crypto Investors Should Pass on Most of Them', *NextAdvisor* (18 April 2022).

34 Deborah R Meshulam, Katrina A Hausfeld, Michael T Boardman, Jonathan M Kinney and Evan North, 'US Department of Justice, aided by cryptocurrency exchanges, seizes over US$3.6 billion in stolen Bitcoin', *DLA Piper* (15 February 2022).

35 Lisa Barrington, 'Financial crime watchdog adds UAE to "grey" money laundering watch list', *Reuters* (4 March 2022).

36 Lina ibrahim and Tariq Alfaham, 'UAE affirms commitment to strengthening AML/CFT efforts following FATF decision', *Emirates News Agency* (4 March 2022).

Some businesses in the UAE are already accepting cryptocurrency payments following new laws to regulate virtual assets.[37] The United Kingdom recently announced that it plans to make a cryptocurrency, stablecoins,[38] a recognised form of payment. Other countries, including the GCC will likely follow suit.

The growing focus on cryptocurrencies will likely lead to multiple attempts to seize such assets, which means seizing illicit funds and helping to prevent the underlying crimes.

Crypto-related crime may be at an all-time high, but legitimate cryptocurrency use far outstrips illegal use.

How much cryptocurrency are crypto criminals holding?

On the other hand, there are legitimate questions relating to how extensive the use of cryptocurrency is in criminal enterprises. Although the answer is impossible to know, an estimate can be made based on the up-to-date list of known addresses that the likes of Chainalysis have identified as being associated with illicit activity.

As of early 2022, criminal addresses possess at least $10 billion-worth of cryptocurrency. The vast majority is held by wallets related to cryptocurrency theft. Addresses associated with darknet[39] markets and scams also contribute to this number. Much of this figure comes not from the initial amount derived from criminal activity but from the ensuing value growth of the crypto assets.

In November 2021; the US Federal Bureau of Investigation (FBI) warned of an increase in bitcoin ATM scams.[40] The FBI highlighted in an alert that it had seen a rise in scams that involved fraudsters directing victims to make payments using bitcoin ATMs and digital QR codes that were popularised during the pandemic. There are static versions of QR codes, meaning that once created, the QR code is permanent and

37 Ian Oxborrow, 'Dubai school says it is first in Middle East to accept cryptocurrencies for fee payments', *The National* (22 March 2022).

38 GOV.UK, 'Government sets out plan to make UK a global cryptoasset technology hub' (4 April 2022).

39 The darknet refers to networks that are not indexed by search engines such as Google. These are networks that are only available to a select group of people and not to the internet public, and are only accessible via specific software.

40 US Federal Bureau of Investigation public service announcement, 'The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment' (4 November 2021).

will always bring users to that content as long as anyone can physically scan it with a smartphone. Static QR codes are best for one-time use because they cannot be edited or tracked.

The FBI noted that it has seen a proliferation of fraud schemes involving payment through bitcoin ATMs, including scams related to online impersonation fraud and romance scams, which continue to develop. The latter is in today's top five crypto scams, as reported in March 2022 by US News.[41]

There are bitcoin ATMs in the UAE and the KSA that service many cryptocurrencies, potentially making these scams a key regional consideration.

Moving forward

Blockchain analysis and computer forensics are not stand-alone offerings: several layers of association are needed to identify bad actors.

Initial success in pursuing crypto crimes have been because of new regulations and the narrowing of know-your-customer standards among entities that deal with traditional currencies. Converting traditional currency to cryptocurrency dramatically dilutes the anonymity of crypto wallets as identification is required at the point of entry. There are also other sources of intelligence and evidence, such as forensically gathering data from seized mobile phones and computers.

Understanding of the blockchain, with its in-built cryptography, the ability to carve addresses from electronic media and the extraction of private keys from wallets, is not typically found among financial investigators. Digital forensic analysts have a different skill set that is more appropriate; however, they may not necessarily understand financial matters associated with money laundering and fraud. This poses the question of whether hybrid crypto investigators are needed.

Regional investigators and stakeholders must develop tools to ensure that interested parties can request GCC authorities to seize digital assets held by cryptocurrency exchanges without issuing mutual legal assistance treaty (MLATs) requests. The seizures will be vital to keep up with the speed of cryptocurrency investigations since MLAT requests (eg, those agreed between the UAE and the United States) are usually lengthy, and cryptocurrency moves almost instantaneously.[42]

41 John Divine, '5 Top Crypto Scams to Watch in 2022', *US News* (22 March 2022).

42 See footnote 31.

One certainty about the future is that any new cryptocurrencies that start to gain traction among clientele, in particular criminals, need to be understood by investigators, where possible, before they form part of an investigation.

Investigative challenges

The particular features of virtual currency systems operating on significantly DeFi systems present new challenges for investigators, both globally and in the GCC. Many of the benefits that cryptocurrency systems promise legitimate consumers, such as increased privacy in transactions and the ability to send funds without an intermediary, serve as obstacles to investigators when the systems are exploited for illegal purposes.

Key challenges identified by investigators dealing with cryptocurrency include regulatory and compliance disparities, transaction obfuscation and anonymity, and the global nature of the systems.

Investigators must standardise and constantly review cybercrime investigative techniques in digital investigations involving DeFi virtual currencies. They may have difficulty getting the information necessary to trace the transaction, especially if the victim uses a wallet service provider or exchanger in an uncooperative foreign jurisdiction or a privacy-orientated cryptocurrency.

Conclusion

GCC countries are seeking to create regulatory regimes covering data privacy, AML/CFT and cybercrime that match the complex environment in which companies operating in those countries find themselves. The changes to these regimes create both challenges and opportunities for corporate investigators.

The heightened use of cryptocurrency by both genuine investors and criminals illustrates the challenges that both corporate and government investigators will face in this evolving landscape. Investigators must stay up to date or bring in the expertise required to future-proof their effectiveness.

DARREN MULLINS
Accuracy

Darren Mullins, who is a partner and head of forensic technology for Accuracy in the Middle East, has 16 years of experience in the fields of digital forensics, electronic discovery, fraud analytics and, more recently, cyber forensics and incident response.

Acting as an expert, he provides the understanding and insights into digital evidence uncovered during cyber and fraud-related investigations and disputes, delivering defensible solutions that take critical evidence from identification and preservation through to presentation and disclosure in the support of internal matters and litigation around the globe.

He has provided confidential expertise to clients operating in the Middle East region for over 10 years and has provided expert testimony in successful litigation and arbitration cases in the DIFC and the United Kingdom.

Prior to joining Accuracy, Darren was a partner at KPMG Lower Gulf and led both Deloitte and EY's forensic technology practices in the Middle East, and he is a regular speaker and chair for industry and government-sponsored conferences in the UAE.

PAUL WRIGHT

Accuracy

Paul Wright is a senior adviser in forensic technology for Accuracy in the Middle East and has 25 years of experience in the fields of cybercrime, incident response, digital forensics, cyber and criminal investigations.

Paul is an extremely accomplished and recognised expert in cybercrime investigations, digital forensics, incident response and cyber fraud risk assessments, with a public and private sector track record of successfully scoping, developing and delivering on investigative engagements for high-profile clients across the globe.

He has expertise in the management of investigations aimed at the highest levels of criminal activity worldwide, which on numerous occasions has resulted in him acting as an expert witness in both criminal and civil courtrooms around the world.

Prior to joining Accuracy, Paul was an associate director with KPMG Lower Gulf and Deloitte Forensic Technology practices in the Middle East.

His previous experience includes serving as detective sergeant in charge of the hi-tech crime team, City of London Police in the United Kingdom and detective sergeant with the UK National Hi-Tech Crime Unit.

WENDY ROBINSON
Accuracy

Wendy Robinson is a senior adviser to the forensic technology team based in Dubai. She has 25 years of experience in the fields of e-discovery and IT project management. She has overseen and delivered innovative applications of e-discovery processes and technology to help clients manage challenging information requests and document reviews. She has used machine learning (AI) tools and workflows for projects, including privilege reviews and personal data carve-outs.

As head of e-discovery, she deployed the first e-discovery platform (Relativity) in the Middle East and North Africa (MENA) region.

Prior to joining Accuracy, Wendy worked at Deloitte, EY and KPMG, leading e-discovery teams in the United Kingdom and MENA. She has led numerous large-scale projects involving data collection, processing, e-discovery hosting, document reviews and standardised productions (eg, for the US Securities and Exchange Commission) across Europe, the Middle East and the United States for clients in the financial services, manufacturing, oil and gas, telecommunications, pharmaceuticals, transport and retail sectors.

RAE LAWRIE
Accuracy

Rae Lawrie is a director in the Dubai office of Accuracy, where he specialises in forensic accounting, fraud, financial and corruption investigations. Rae has over 26 years of experience in undertaking these types of assignments in support of civil litigation and arbitration proceedings. He is a fellow of the Association of Chartered Certified Accountants and has over 10 years of law enforcement experience with the UK Serious Fraud Office. Since 2004, Rae has provided investigative and forensic accounting services to corporate clients from across the globe.

His expertise includes conducting large-scale, criminal and civil litigation and arbitration assignments related to fraud and corruption-related and multi-jurisdictional asset tracing and regulatory investigations on behalf of clients and regulators in Europe, Middle East and the Americas.

Prior to joining Accuracy in February 2020, Rae gained extensive experience with Deloitte and KPMG in London and the Middle East.

Accuracy is a wholly independent professional advisory firm that provides advice to company management and shareholders for their strategic or critical decisions, notably in transactions, investigations, disputes and crises. Accuracy regularly provides services to leading international law firms and companies, including over 50 per cent of France's CAC40 companies.

Accuracy is one worldwide partnership with 18 offices in 13 countries across Europe, the Middle East, Asia, Africa and North America. Our teams speak over 35 languages, even while maintaining one company culture with shared values and principles, including upholding the strictest ethical standards and avoiding any conflicts of interest.

Accuracy's investigations and forensic services team brings together professionals with a wealth of backgrounds and competencies, including forensic accountants, finance professionals, corporate investigators, data analysts, technologists and former government enforcement authorities and investigations attorneys. These diverse backgrounds allow Accuracy to take a cross-disciplinary approach to investigations and other risk-based services, including forensic accounting, e-discovery, due diligence, corporate intelligence, asset tracing and compliance reviews.

The firm's investigators have a deep understanding of business and finance, allowing them to find financial misconduct more easily than those with a more narrow training or focus on accounting. Further, Accuracy uses a combination of proprietary and innovative technological solutions as part of its investigations practice, recognising that technology is often critical in both assessing new allegations and resolving matters as quickly as possible.

Dubai International Financial Centre
Index Tower, Level 14, Office 1402
PO Box 506647
Dubai
United Arab Emirates
Tel: +971 4 3736 901
www.accuracy.com

Darren Mullins
darren.mullins@accuracy.com

Paul Wright
paul.wright@accuracy.com

Wendy Robinson
wendy.robinson@accuracy.com

Rae Lawrie
rae.lawrie@accuracy.com

EPPO and Investigations in Romania in Covid Times

Horia Draghici, Mihai Jiganie-Serban and Cosmin Cretu
CMS Cameron McKenna Nabarro Olswang LLP

IN SUMMARY

This article provides insight into the activity and jurisdiction of the European Public Prosecutor's Office and the investigative actions taken by the Romanian authorities during the covid-19 pandemic.

DISCUSSION POINTS

- EPPO's first annual activity report
- Investigations in the context of the pandemic
- Covid-19 aids during the state of emergency
- The National Anti-Corruption Directorate's activity report for 2021
- The National Recovery and Resilience Plan 2021
- Anticipated developments

REFERENCED IN THIS ARTICLE

- EPPO
- National Anti-Corruption Directorate
- Court of Accounts report on public sector acquisitions during the state of emergency
- Unifarm SA
- EPPO's first annual report
- The National Anti-Corruption Directorate's activity report for 2021
- The European Commission
- The National Recovery and Resilience Plan 2021
- European Anti-Fraud Office

EPPO

The European Public Prosecutor's Office (EPPO) started operations on 1 June 2021. The EPPO is an independent and decentralised prosecution office of the European Union, with the competence to investigate, prosecute and bring to judgment crimes against the EU budget, such as fraud, corruption and serious cross-border VAT fraud.[1]

The EPPO is built on two levels: strategic and operational.

- The strategic level comprises the European Chief Prosecutor (assisted by two deputies), who works alongside the College of Prosecutors – one from each participating member state.
- The operational level is represented by European delegated prosecutors (at least two in each participating member state) who are responsible for investigating, prosecuting and bringing to judgment cases falling within the EPPO's competence. In their investigations and prosecutions, the delegated prosecutors are monitored and directed by permanent chambers, which will take operational decisions.

So far Romania has appointed seven European delegated prosecutors, all of whom were accepted by the EPPO.

The EPPO will have jurisdiction to investigate, prosecute and bring to judgment the following crimes against the EU budget:

- fraud – the use or presentation of false or incorrect information or the withholding of required information, which leads to the wrongful retention of EU funds or assets, or the diminution of EU resources. Regarding VAT fraud, the EPPO will only be competent if the misconduct relates to at least two participating member states and has caused a total loss of at least €10 million;
- corruption – both active and passive;
- misappropriation of EU funds – disbursement of funds by a public official contrary to their intended purpose and thus damaging the EU's financial interests; and
- money laundering involving the proceeds of crimes against the European Union's financial interests.

The EPPO's jurisdiction will also extend to (1) offences regarding participation in a criminal organisation of which the focus is to commit any of the offences against the European Union's financial interests and (2) any other crime inextricably linked to the commission of crimes against the European Union's financial interests.

1 More information on the EPPO can be found on the website of the European Commission.

Before the creation of the EPPO, frauds regarding EU funds were investigated by the National Anti-Corruption Directorate (DNA). The EPPO is set to take over an impressive number of files that are currently being investigated by the DNA that probe corruption offences (eg, bribery, influence peddling and abuse of office) and all types of crimes committed against the financial interests of the European Union.

According to the chief prosecutor of the DNA, the EPPO is set to take over around 500 to 600 criminal investigation files from the DNA, assuming the EPPO will only take over files with damages exceeding €100,000. In addition, the EPPO will take over the cross-border tax evasion files, which are under investigation by other competent prosecution offices.

According to the EPPO's first annual report,[2] there are 44 active investigations in Romania with estimated total damages of €1.3 billion. Most reports and complaints (336) came from the national authorities. Seven reports came from EU institutions, bodies, organisations and agencies, and only 10 reports came from private parties. Following these reports, in 291 cases the EPPO took the decision not to exercise competence; only in 60 cases did it decide to exercise its competence.

The countries with the most active EPPO investigations are Italy (102 active investigations), Germany (54 active investigations), Slovakia (42 active investigations), the Czech Republic (34 active investigations) and France (29 active investigations). Although to date no major EPPO investigation has made the headlines in Romania, eight cross-border EPPO investigations involved Romania since either part of the acts had been committed in Romanian territory or Romania had also suffered damage owing to the unlawful activities.

Regarding cross-border investigations, the principal challenges that arise relate to:

- difficulties in coordinating the investigation efforts across cultures and in communicating effectively in different languages;
- differences in laws regarding attorney–client privilege, employee rights and data protection laws across various countries; and
- differences in the attitudes and approaches of the law enforcement authorities.

2 European Public Prosecutor's Office, 'The EPPO investigates €5.4 billion worth of loss to the EU budget in its first 7 months of activity' (24 March 2022).

Certain challenges may also arise owing to the over-criminalisation of certain, non-violent acts, such as the offence of influence peddling incriminating the simple promise to persuade a Romanian public official to act in a certain way, irrespective of whether an undue advantage was pursued or whether the supposed influence was exercised abusively.

Investigations in the covid-19 context

The Romanian authorities continued their enforcement efforts in respect of allegations of corruption in the healthcare sector in 2021, especially in the context of the covid-19 pandemic. Given the supply and demand of medical devices used for protection and sanitary materials and the weak oversight of the authorities owing to the health systems being on the brink of collapse, certain individuals took advantage of the situation and used public money to enrich themselves.

According to an article by Digi24 about the management of public resources during the state of emergency (March to May 2020),[3] the Court of Accounts announced that the estimated financial and accounting deviations for the said period amount to 659 million Romanian lei (approximately US$144 million), and the damages amount to 38.3 million Romanian lei (approximately US$8.4 million).

The expenses made to fight the pandemic until 30 June 2020, from the state budget, local budgets and the unemployment insurance budget amount to 5 billion Romanian lei (approximately US$1.1 billion) of which:

- 73 per cent represents the payment of the allowance granted during the suspension of the individual employment contract at the initiative of the employer (3.69 billion Romanian lei – approximately US$810 million);
- 13 per cent represents the allowances granted to other categories of staff whose activities were interrupted or took place at a very low level (662 million Romanian lei – approximately US$145 million); and
- 5.3 per cent represents the expenses regarding the medical emergency reserves (266 million Romanian lei – approximately US$58 million).[4]

During the state of emergency, the Ministry of Health bought the medicines, medical devices and sanitary materials used in the fight against the covid-19 virus by means of the state-owned company Unifarm SA (Unifarm). The budget of Unifarm for 2020

3 'RAPORT privind starea de urgență: Curtea de Conturi a găsit prejudicii în gestionarea banului public de 38,3 milioane de lei', *Digi24* (11 August 2020).

4 Court of Accounts, 'Gestionarea resurselor publice în perioada stării de urgență' (August 2020).

was increased by 1.15 billion Romanian lei (approximately US$250 million) for this purpose. Part of those acquisitions have been investigated by the DNA and led to the indictment of the former director of Unifarm for alleged corruption and breach of public procurement rules.[5]

Although the speed of investigations at the DNA has been reduced by the restrictions imposed by the authorities in during the pandemic, the DNA managed to conclude several high-profile investigations.

In October 2020, DNA prosecutors indicted the former director of Unifarm for bribery, abuse of office and influence peddling allegations surrounding the conclusion of a contract for the delivery of protective equipment during the pandemic. According to the DNA prosecutors,[6] the former director of Unifarm requested €760,000 from an intermediary representing a private company for the award of a contract for the purchase of 250,000 hazmat suits and 3 million surgical masks, in breach of public procurement rules.

Together with the former director, the DNA prosecutors also indicted the former head of commercial services at Unifarm, who allegedly unrealistically attested on the awarding documentation the fact that the negotiation was carried out with the legal representative of the private company, when in fact the negotiation took place between the former director of Unifarm and the intermediary at a restaurant in Bucharest.

According to the prosecutors, for this activity, the intermediary requested 18 per cent of the contract value (ie, 5,810,175 Romanian lei – approximately US$1.2 million), of which €760,000 would go to the former director of Unifarm.

The prosecutors further claim that the former director of Unifarm decided to unilaterally terminate the contract because the private company failed to pay the requested amount to the intermediary, despite the fact that the latter delivered part of the products. The damage caused to Unifarm amounts to 2.38 million Romanian lei (approximately US$520,000) – the value of the products delivered by the private company, part of which did not observe the standards mentioned in the contract.

According to a DNA press release dated December 2020,[7] the former director of Unifarm is also under investigation for abuse of office as he allegedly awarded a private company with a 4.5 million Romanian lei (approximately US$1 million) contract for the purchase of 1.5 million three-ply surgical masks, in breach of public procurement rules.

---

5 National Anti-Corruption Directorate (DNA) Press Release No. 648/VIII/3 (2 October 2020).

6 ibid.

7 DNA Press Release No. 828/VIII/3 (4 December 2020).

The prosecutors claim that although the private company had not been approved by the National Agency for Medicines and Medical Devices for the import and distribution of three-ply surgical masks at the date of concluding the contract, two days after conclusion, Unifarm's director made an advance payment of 3.6 million Romanian lei (approximately US$790,000). At the date of the press release, the company did not deliver any masks, and after the termination of the contract it failed to return the amount received as an advance payment.

The former director of Unifarm may also be subject to another investigation for alleged fraud, abuse of office and making false statements in connection with the acquisition of medical masks during the state of emergency.[8] Judicial sources claim that the case concerns the acquisition by Unifarm of 1.2 million masks from a private company. The masks were distributed in hospitals throughout Romania but were later withdrawn owing to issues reported by medical staff. The masks were also subject to an alert at the European level owing to their low filtering capacity.

Covid-19 aids during the state of emergency

During the state of emergency, the government issued legislation supporting employers that needed to suspend the employment contracts of their employees owing to the pandemic by bearing 75 per cent of the employees' gross salary (but not more than 75 per cent of the average gross salary at the national level).

Over 1 million employment contracts are reported to have been suspended owing to the pandemic between March and May 2020. This has translated into a large number of applications for state support during the technical unemployment period.

The Romanian authorities announced controls and severe sanctions for employers that may have illegally claimed (and obtained) technical unemployment support offered by the government in the context of the pandemic.[9] These controls may materialise in the form of notifications to the competent criminal investigation authorities, as announced by the Ministry of Labour and Social Protection at the time.[10]

---

8 Sebastian Pricop, 'Dosar penal privind măștile neconforme achiziționate de Unifarm', *Europa Liberă România* (3 February 2021).

9 Cristian Pantazi and Cristian Citre, 'Unii angajatori încearcă să fraudeze ajutorul de stat pentru șomajul tehnic. Violeta Alexandru: Cine face declarații false pe propria răspundere riscă dosar penal', *G4 Media* (10 April 2020).

10 Mihai Jiganie-Serban and Cosmin Cretu, 'Potential criminal liability for employers who illegally claimed technical unemployment support', *CMS Law Now* (14 May 2020).

According to the Ministry, the main focus seemed to be on the companies that, despite having applied for technical unemployment support, did not in fact interrupt their activity during the state of emergency and requested their employees to come to work. In other cases, there were suspicions that employers may have submitted the same application with authorities from different counties to receive multiple payments.

In addition to returning any illegally obtained amounts to the state, companies that illegally applied for the technical unemployment support from the state may also face criminal law sanctions.

Considering that the costs from the Unemployment Social Contributions Budget were covered by European non-reimbursable funds, if the companies were not eligible to apply for the aid, the director or the legal representative of the companies, as well as the companies themselves, may be held criminally liable for unlawfully obtaining European funds, which is punishable by up to 14 years' imprisonment for individuals and a maximum fine of 3 million Romanian lei (approximately US$658,000) for the companies. Such crimes fall within the EPPO's jurisdiction.

DNA's activity report for 2021

According to the DNA's activity report for 2021,[11] 175 criminal files have been registered since the beginning of the state of emergency (ie, 16 March 2020) in connection with the covid-19 pandemic. The DNA finalised 27 cases, issuing seven indictments (in respect of 19 individuals) and concluding four guilty plea agreements. In December 2021, the DNA still had 89 active cases concerning the pandemic under investigation.

The number of DNA investigations relating to the pandemic increased in 2021, given that only 33 criminal cases had been registered in May 2020.[12] These investigations revealed:

- breaches of legal provisions for the organisation, award and performance of direct public procurement contracts for protective equipment (masks, face coverings and hazmat suits);
- purchases of non-compliant masks that are deemed dangerous and prohibited in the European Union; and
- unlawful establishment of quarantine centres and assignment of people to quarantine centres.

11 The DNA 2021 Activity Report can be found on the DNA's website.

12 DNA Press Release No. 294/VIII/3 (21 May 2020).

In a detailed interview dated June 2020,[13] in respect of public procurement, the chief prosecutor of the DNA stated that the prosecution office was taking a close look at both public procurement relating to the pandemic and public procurement in general. This is because, in respect of the latter, public procurement also took place in other areas where crime is suspected of being perpetrated.

In this respect, at the date of this interview, the DNA had registered 38 criminal files concerning alleged breaches of public procurement rules with undue benefits for certain people and the alleged purchase of goods that do not comply with EU requirements or with those of their destination.

The value of the contracts under investigation by the DNA at the date of the interview amounted to 800 million Romanian lei (approximately US$175 million). The chief prosecutor of the DNA stated that damages in acquisitions of non-compliant goods amount to the total value of the contracts, while the damages in corruption allegations (eg, bribery and influence peddling) or crimes related to those of corruption (eg, abuse of office) are between 5 per cent and 18 per cent of the contract value (the damages in each of those files ranges between €400,000 and €4 million.

National Recovery and Resilience Plan 2021

The European Commission adopted a positive assessment of Romania's recovery and resilience plan,[14] under which the country will receive €14.2 billion in grants and €14.9 billion in loans under the EU Recovery and Resilience Facility (RRF).

The RRF is the key instrument of NextGenerationEU, the European Union's covid-19 recovery plan and the Multiannual Financial Framework, the European Union's long-term budget.[15]

The National Recovery and Resilience Plan (NRRP) is structured into the following six pillars: green transition; digital transformation; smart growth; social and territorial cohesion; health and economic, social and institutional resilience; and policies for the next generation, children and youth.

13 Ioana Ene Dogioiu, 'Crin Bologa, șef DNA, despre repornirea anticorupției: Avem dosare importante cu persoane și prejudicii importante. Nu fac compromisuri! - Interviu video', *spotmedia.ro* (15 June 2020).

14 Ministry of European Funds, 'Planul Național De Redresare Și Reziliență (Pnrr)'.

15 'COVID-19 and EU budget: Recovery and Resilience Facility Regulation published in Official Journal', *Thomson Reuters* (18 February 2021).

Thirteen of the 21 milestones and targets that the government had to meet by 31 December 2021 were met.[16] So far, Romania has received €3.7 billion under the NRRP. Romania will have to follow tight restrictions regarding spending the €30 billion it will receive in line with the provisions set by the European Union: at least 40 per cent must be for green projects and more than 20 per cent must be for digitisation.[17]

Investments in natural gas infrastructure were also accepted as being eligible after several countries, including Romania, pressed for this. The €30 billion will be divided as follows: 40 per cent as soft loans and 60 per cent as grants.

According to a member of the European Parliament,[18] the projects submitted by local authorities through the National Local Development Programme can be funded by the NRRP if they comply with European rules. Projects with feasibility studies, which are not financed by other European funds, can be included in the NRRP if the works will be carried out in the future or were carried out from 1 February 2020.

A Bucharest mayor stated that he had completed the legal procedures and submitted projects amounting to over €117 million for financing through the NRRP.

Investments financed under this plan must start by 2024 and be completed by 2027.

Anticipated developments

According to the 2019 report of the European Anti-Fraud Office (OLAF), Romania is the member state with the highest number of investigations into the use of EU funds managed or spent in whole or in part at the national or regional level in 2019. More than 10 per cent of the total number of OLAF investigations in 2019 were conducted in respect of EU funds spent in Romania.

Romanian authorities are expected to continue their enforcement efforts in respect of allegations of corruption in the healthcare sector in 2022, especially given the pandemic and the need to allocate funds to procure medicines and medical devices.

16 Andrei Chirileasa, 'Author of RO Resilience Plan says 4 of 21 milestones for end-2021 are at risk', *Romania Insider* (11 January 2022).

17 Andrei Chirileasa, 'Romania must submit Recovery and Resilience Plan to the EC this month', *Romania Insider* (17 February 2021).

18 Ramona Cornea, 'Ce înseamnă Planul Naţional de Redresare şi Rezilienţă pentru comunităţile locale? Proiectele depuse în PNDL pot fi finanţate prin Programul Naţional de Relansare şi Rezilienţă, dacă respectă regulamentul european', *Ziarul Financiar* (4 March 2021).

Given the large amount of European funds that went or are going to many EU countries, including emerging members such as Romania, as aid to combat the covid-19 virus or as part of the Recovery and Resilience Facility, the EPPO will have the authority to investigate alleged misconduct regarding the way the European funds are spent during the pandemic and beyond.

HORIA DRAGHICI
CMS Cameron McKenna Nabarro Olswang LLP

Horia Draghici is a partner in CMS Bucharest's dispute resolution team. With over 17 years' experience, Horia has a great deal of experience in commercial litigation for both multinational clients and significant domestic companies in Romania, including experience with the International Centre for Settlement of Investment Disputes.

Horia has a natural ability to understand and explain cases in detail and inspire high levels of confidence in clients. His practice deals extensively with commercial litigation and arbitration, insolvency matters, disputes with public authorities and international investments disputes. Horia is qualified to plead before all national courts (including the High Court of Romania) and is a skilled negotiator, who is familiar with several alternative dispute resolution techniques.

MIHAI JIGANIE-SERBAN
CMS Cameron McKenna Nabarro Olswang LLP

Mihai Jiganie-Șerban is a senior counsel and head of the criminal law practice of CMS in Romania, specialising in criminal law, regulatory and compliance. With over 17 years' legal experience, Mihai focuses on criminal law, with significant experience advising on anti-corruption, economic crimes, money laundering cases and capital market and pharma industry fraud. Mihai has advised national and international companies on legal-framework issues, internal investigations and representation before the state authorities.

Throughout his career, he has successfully assisted and represented both individuals and national and international companies across a diverse range of industries, including oil and gas, banking and finance, leasing, insurance, energy, civil and industrial constructions, and media and advertising. He has represented clients in front of all structures of the public authorities (police, prosecutors' offices and courts of law).

COSMIN CRETU
CMS Cameron McKenna Nabarro Olswang LLP

Cosmin Cretu is an associate in the CMS Bucharest team, specialising in criminal law, regulatory and compliance. Cosmin has broad experience in criminal defence of companies and senior executives facing various white-collar crime allegations. He has been advising multinational companies operating in the energy, IT, life sciences, construction and infrastructure, automotive, banking and insurance sectors facing allegations of tax evasion, money laundering and corruption with claimed damages exceeding €500 million. Cosmin has been conducting internal investigations, and he regularly assists clients before prosecuting authorities and courts of law in various criminal law disputes.

Cosmin also focuses on a wide range of compliance and regulatory matters relevant to the gambling, life sciences and TMT sectors. Prior to joining CMS, Cosmin was a senior associate at a top-tier law firm specialising in white-collar crime.

CMS provides clients with specialist, business-focused advice on law and tax matters. With our 4,500 legal professionals across the world, working in sector-based teams and expert in project management, our focus is on our clients and fulfilling their objectives. CMS is a full-service top 10 global law firm, based on the number of lawyers (Am Law 2018 Global 100).

CMS provides a wide range of expertise across 19 expert practice and sector areas, including banking and finance, commercial, competition, corporate, dispute resolution, white-collar crime, employment, energy, funds, intellectual property, life sciences/ pharmaceuticals, real estate and construction, tax and TMT.

CMS has a 60-lawyer office in Bucharest, along with over 70 offices in over 40 countries, and an anticorruption and investigations team comprising 13 lawyers. Given the crackdown on corruption in recent years, the firm has developed a major focus on white-collar crime and a strong criminal defence practice in Romania, representing multinational business groups in anti-corruption investigations, fiscal fraud investigations, compliance counselling and business-critical criminal investigations.

The team regularly advises multinational corporations in regulatory, investigative and contentious matters in relation to anti-corruption and white-collar crime, including anti-corruption investigations and enforcement, fiscal investigations, compliance counselling, whistle-blower claims, procurement fraud, antitrust violations and securities enforcement.

One Tower 165 Calea Floreasca
District 1
014459 Bucharest
Romania
Tel: +40 21 40 73-800
Fax: +40 21 40 73-900
www.cms.law

Horia Draghici
horia.draghici@cms-cmno.com

Mihai Jiganie-Serban
mihai.jiganie-serban@cms-cmno.com

Cosmin Cretu
cosmin.cretu@cms-cmno.com

Corporate Anti-Corruption Enforcement Trends in Russia

Paul Melling and Roman Butenko
Baker McKenzie

IN SUMMARY

In recent years, Russia has tried to streamline its corporate anti-corruption enforcement to make it more predictable and to take into account best practices across the globe. Without minimising the scale of the problem that Russia faces in achieving those objectives, this article provides an overview of recent corporate anti-bribery enforcement trends and, taking into account those trends, tries to sum up the most important lessons to be learnt by companies that strive to build compliant businesses in Russia.

DISCUSSION POINTS

- Russian corporate anti-corruption enforcement must be taken into account by companies, especially those with an international footprint and those that actively participate in Russian state tenders
- Small and medium-sized businesses remain under the biggest enforcement exposure, but law-enforcement has made attempts to switch the focus to bigger companies
- Both legislation and enforcement practice enable prosecution of companies for bribery offences committed by parties with extremely remote connections to the accused legal entity
- The nature of the anti-corruption offences detected reinforces the need for proper compliance training of employees
- Corporate compliance programmes gain more weight as a potentially successful defence in anti-corruption enforcement cases

REFERENCED IN THIS ARTICLE

- Code of Administrative Offences
- Law on Combating Corruption

In Russia, as in many other countries, companies are subject to liability for their corrupt activity. At first sight, Russian financial penalties for corporate bribery may not appear as significant as, for example, in the case of the potential liability for violations of the US Foreign Corrupt Practices Act or the UK Bribery Act; however, this is not a reason not to prioritise compliance with Russian anti-corruption legislation. There are a number of reasons why this continues to be a hot topic for the majority of international companies operating in Russia.

First, in Russia it is the courts that are empowered to prosecute for corporate bribery. Court judgments are publicly available and can be easily accessed by foreign law enforcement authorities that could consider prosecution in Russia as a trigger for opening their own investigation with a broader scope and potentially much more severe consequences.

Russian mass media and prosecutors contribute to the public circulation of information on anti-corruption enforcement cases; thus, even where judgments are unavailable or difficult to find, there is still likely to be plenty of information in the public domain about those cases.

Second, companies prosecuted for corporate bribery offences are not allowed to participate in state procurement tenders for a certain period. State procurement has traditionally been an important part of the Russian economy, and potential debarment from state tenders is a critical concern for many companies that directly or indirectly have the government as their biggest customer enterprise (eg, life sciences companies).

Third, Russian legislation is well designed to prosecute companies for bribes given on their behalf, in their name or in their interests, even where the company is wholly unaware of the bribe being paid and did nothing to encourage it. As cases like this start to appear, companies are beginning to pay more attention to introducing controls for the choice of and interaction with their counterparties.

Last but not least, although most fines for corporate bribery offences are comparably small, they may be quite significant – even for big companies. The amount of the fine depends on the amount of the bribe and could reach 100 times that amount. So far, the biggest fine imposed on a company in Russia reached 100 million roubles, but we expect that this record will be beaten in the coming years.

Enforcement trends in brief

The overall state of corporate anti-corruption enforcement in Russia has been more or less stable over recent years. No major game changers have appeared in legislation or enforcement practice.

Small and medium-sized businesses remain under the biggest enforcement exposure for a number of reasons:

- they tend to have a less significant compliance culture, less funds to establish compliance controls and an inadequate understanding of how they can benefit from being compliant;
- they operate at the regional or local level, where corruption is somewhat more inherent and can be part of everyday business life; and
- they are put under pressure by their bigger counterparties and have to find ways to survive and be profitable against the backdrop of decreasing income of the population and various crisis situations, such as the covid-19 pandemic.

This does not mean that large Russian companies and multinationals are given a free ride by the enforcement authorities. On the contrary, the enforcement focus has started to move towards a more advanced anti-corruption environment, similar to the environments foreign companies are used to in other jurisdictions.[1] This is reflected in a number of mutually related trends.

First, Russian law enforcement authorities have become more and more interested in bigger fish instead of commencing numerous low-profile cases. Russian legislation has changed to accommodate this objective. The covid-19 pandemic has only reinforced this trend as the sentencing of higher fines to restore the budget and the abilities of law enforcement to initiate numerous low-profile cases has been affected by the pandemic-related lockdowns and various subsequent restrictions.

Second, Russian courts have started to pay more attention to corporate compliance programmes (and the adequacy thereof, both on paper and in practice) when it comes to the issue of imposing liability for bribery offences.

These trends reflect the growing demand for compliant business practices and for the introduction of strengthened and targeted compliance controls.

In this article, we provide a more detailed overview of the state of corporate anti-corruption enforcement and recent trends and seek to identify lessons to be learned by companies striving to build a compliant business in Russia.

1 Baker McKenzie, 'Russia: Corporate Anti-Corruption Enforcement Trends'.

Overview of legislation

The provision prohibiting bribery by companies is contained in article 19.28 of the Code of Administrative Offences (the Administrative Code). It provides very broad grounds for the liability of legal entities for bribery offences. It prohibits the mere offer or promise of a bribe by a person acting in the name or in the interests of a legal entity.

In particular, article 19.28 prohibits the following:

> *Unlawful provision, offer or promise made in the name or in the interests of a legal entity or in the interests of a related legal entity of monies, securities or other property, rendering services of a pecuniary nature or provision of property rights to a public official, an official with management functions in a commercial or other organization, a foreign public official or an official of a public international organization (including when upon instructions of the public official, the official with management functions in a commercial or other organization, the foreign public official or the official of a public international organization monies, securities or other property are transferred, offered or promised, services of pecuniary nature rendered or property rights provided to another individual or a legal entity) for any act or omission in connection with his/her duties of office, committed by the public official, the official with management functions in a commercial or other organization, the foreign public official or the official of a public international organization in the interests of this legal entity or a related legal entity.*

Liability for bribery under article 19.28 can reach 100 times the amount of the bribe (if the bribe exceeds 20 million roubles). As far as we are aware, the largest fine in the history of article 19.28 enforcement was levied by a court of first instance in 2019, which imposed total penalties of 155.9 million roubles, including a fine of 100 million roubles and 55.9 million roubles in confiscated illegal payments. The district court subsequently decreased the fine to 50 million roubles, but even so it remains the record holder.

Other top fines vary from 100 million roubles to 20 million roubles.

Article 19.28 can be applied to offences committed outside Russia, and in 2019 we saw such a case for the first time, that case involving an official from Belarus.

Administrative proceedings under article 19.28 are initiated by the prosecutor's office, after which the case is transferred to court to decide whether the company will be held liable. The courts of first instance for those cases are the magistrates' courts. The majority of magistrates still have insufficient experience with cases under this article; many find themselves considering cases under this article for the first time.

While the rulings of the magistrates' courts may be appealed to a number of higher courts, including the Supreme Court, in our experience, higher courts rarely repeal or change the rulings of magistrates' courts in this category of cases.

Russian legislators periodically make amendments to article 19.28 and related laws in accordance with developing international best practices in countering corporate corruption. The most relevant among the recent changes are as follows.

- In mid-2018, article 19.28 was supplemented with note 5, which provides a basis for relief from liability in the event of cooperation with law enforcement bodies in detecting and investigating offences, as well as in the event of extortion of illegal payments. The amendments also envisage the possibility of arrest of property or funds of a company to guarantee execution of a court ruling.
- At the end of 2018, amendments were introduced into article 19.28 allowing a company to be prosecuted, even in the absence of the company's interest in the commission of an offence, if the offence was committed in the interest of a 'related legal entity' (this concept is not defined in the law). Furthermore, the recipient of the illegal reward need not be an official but can also be any third party on the instructions of an official.
- At the end of 2019, amendments were made to the Administrative Code allowing the term of an administrative investigation for cases under article 19.28 to be extended by up to 12 months in cases involving a request for legal assistance sent to a foreign state.

In addition, in the summer of 2020, the Supreme Court published an overview of court practice in cases involving article 19.28. In the overview, the Supreme Court confirmed the possibility of prosecuting companies under article 19.28 for the actions of third parties not linked to the company by employment, contractual or other legal relations.

Following the letter of the law, Company A can be found guilty of infringement of article 19.28 of the Administrative Code, even when the illegal reward on its behalf was provided, offered or promised by an employee of Company B, if the court considers that the employee acted in the interests (or on behalf) of Company A, whether by agreement between those companies or on some other basis.

Russian court practice has already seen cases in which courts have prosecuted companies under article 19.28, even when the bribe giver had, in our view, an extremely remote connection with the accused legal entity or the court failed to identify a bribe

giver; however, until the publication of the Supreme Court's overview, there was no official guidance on the criteria or basis for holding a company liable for the actions of such third persons.

As the Supreme Court explained, one of the conditions for bringing such charges against a company is the presence of instructions, knowledge or approval by authorised persons of the company of the commission of the actions. Another essential condition for bringing charges is an 'economic or other (for instance, reputational) interest' in the commission of the illegal action.

The below enforcement overview covers legal practice in the past couple of years. Our preliminary review of the cases in the register for 2021 to 2022 confirms the trends outlined below.

Overall state of legal practice in the application of article 19.28

According to statistics published by the Supreme Court, from 2013 to 2017 there was a steady growth in prosecutions under article 19.28, from 164 cases in 2013 to 477 cases in 2017.

There was an insignificant decrease in 2018, and from 2019 to 2020 this decline continued: the number of cases fell to 322 in 2020.

The reasons for this reduction are not entirely clear; a number of factors could have played a role.

First and foremost, an overall change in the focus of law enforcement authorities in anti-corruption cases could have led to this decline. The vast majority of cases under article 19.28 are based on materials collected in the course of criminal prosecutions of individuals; therefore, the number of cases under article 19.28 may be dependent on the level of activity of law enforcement authorities in Criminal Code bribery cases.

According to data from the Judicial Department of the Supreme Court, in 2019 the number of individuals charged in cases of small-scale bribery (cases in which the bribe was less than 10,000 roubles) fell by 31.5 per cent compared with the previous year. At the same time, cases involving illegal payments of less than 10,000 roubles made up more than 39.7 per cent of the total number of cases initiated under article 19.28 in that year. In the following years, around the same figures were recorded.

The decreased interest of law enforcement authorities in prosecuting corruption offences with a bribe below 10,000 roubles is bound to have an effect on the number of cases initiated under article 19.28.

Second, we assume that in 2019 the implementation of note 5 to article 19.28 gathered speed, allowing companies to avoid liability by assisting with the detection and investigation of violations and therefore impacting the figures for 2019 and thereafter.

As far as we know, there is no one publicly available source of information concerning article 19.28 cases that were not brought on the basis of note 5; however, analysing the available information on practice under article 19.28, we see an increase in those cases, which could also partially explain the overall reduction in cases brought under article 19.28.

A decision on the use of note 5 can be taken by the prosecutor when deciding on initiating proceedings under article 19.28; therefore, in most cases, information about those decisions would not come into the public domain and would not be included in the official statistics on article 19.28 enforcement.

In our view, the reduction in the number of cases brought under article 19.28 in 2019 could be the result of an overall improvement in legal practice and a long-awaited refocusing of attention by law enforcement on more significant crimes. The covid-19 pandemic that started in early 2020 contributed to the overall trend by making it difficult for the law enforcement authorities to initiate new cases. This likely explains why the prosecution figures stabilised at around the same level as those in 2019, without any significant growth.

Enforcement highlights and trends

Most prosecutions result from reporting of government officials about an attempt of bribery

The prosecutor's office has the exclusive right to initiate proceedings under article 19.28.

According to our research, in the majority of cases, article 19.28 violations are detected when officials report offers of bribes and as a result of investigative operations: those two categories make up about 95 per cent of cases for which data on the method of detection is available.

More than half of those cases are instances when investigative steps are taken by law enforcement after receiving information that an illegal reward has been offered or promised. Somewhat rarer are investigations conducted at the initiative of the law enforcement bodies (ie, without receiving information on illegal inducements being offered or promised).

There are also cases where the basis of the accusation was a report or an audio recording made by an official of a person offering an illegal reward, in which case there was no separate law enforcement investigation.

This suggests that most of the article 19.28 offences detected arose owing to companies, or parties acting on their behalf or in their interests, proposing bribes (as opposed to officials requesting bribes).

Even vague proposals to come to an agreement can be interpreted by law enforcement as a violation of article 19.28. This highlights the growing need for complete and timely training and provision of information for employees and others acting on behalf of companies about the risks of liability. Specifically, those persons should be instructed that even a proposal or promise to give an illegal reward can have significant negative consequences for the company.

In the event of extortion of an illegal payment by an official, or upon receiving hints from an official about the possibility of an 'informal' resolution of issues, employees should immediately issue an unambiguous refusal to engage in any illegal behaviour and should document the refusal immediately upon closure of the conversation or meeting via internal meeting note or internal report.

Law enforcement tends to focus on bigger bribery cases, but risks of smaller bribery should not be underestimated.

In 2018, in most cases, companies prosecuted under article 19.28 were for relatively small illegal payments. Less than 6 per cent of accusations involved illegal payments of more than 1 million roubles, and around 40 per cent of cases were initiated based on illegal payments of no more than 3,000 roubles.

From 2019 to 2020, the statistics changed significantly. The proportion of cases involving illegal payments of less than 100,000 roubles dropped noticeably from 64.4 per cent to 56.3 per cent of all cases, and the largest increase took place in cases with an illegal payment of more than 2 million roubles. In 2018, there were only six such cases, whereas in 2020 the number more than tripled to 22.

There was a significant increase in the amount of the average illegal payment. In 2018, it was 355,702 roubles, but in 2020 it was more than 733,000 roubles (ie, roughly twice the size). The median bribe grew from 50,012.50 roubles in 2018 to 80,000 roubles in 2019.

Despite this growth in the size of illegal payments under article 19.28, the proportion of cases involving an insignificant illegal payment, as before, remains large. An illegal payment of less than 100,000 roubles was encountered in more than half of all cases in 2020; thus, although law enforcement appears to be shifting its focus to major offences, this should not be seen by companies as a reason to relax controls over smaller expenditures.

Cash bribes are by far most common

In most cases, illegal payments are made in cash, which underscores the need for companies to tighten their relevant controls. In other cases, illegal payments or inducements are made via money transfers, including rapid transfers using a telephone number, the transfer of property or provision of material services.

Bribery through gifts often implies a relatively low monetary value. Recent examples include a bottle of cognac, a crate of paper, a truckload of pit gravel, payment of air tickets to a resort and accommodation in a hotel.

Police officers are the most common bribe-takers, while senior corporate executives are the most frequent bribers

In the period under review, companies most often faced charges for illegal payments offered to police officers. Other frequent recipients of illegal rewards were officials of state institutions and enterprises authorised to take decisions on state procurement, as well as also officials of regional state bodies and the recipients of commercial bribes.

Also among the more common recipients of illegal payments in the period under review were officials of municipal authorities and the Federal Bailiffs' Service, as well as employees of Russian Railways, although figures for both of these categories have slightly declined over the years.

In 2019, and for the first time, there was a case of bribery of a foreign official: an official of the State Aviation Emergency Rescue Institution of the Ministry of Emergency Situations of Belarus. As far as we know, this was the first such case in the history of article 19.28 enforcement, and we have not identified any other cases of that kind since then.

As far as the participants in corruption on the side of the bribe-giving companies are concerned, cases tended to involve top managers: founders, general directors and financial and executive directors. Other company employees and persons not formally linked to companies by employment or other legal relationships were involved much less frequently.

Companies should pay particular attention to interactions in the course of state procurement

Most frequently, companies face potential liability for illegal rewards designed to ensure a certain decision is taken and for cooperation in obtaining commercial contracts, including as part of state procurement processes.

Companies often give or offer bribes for decisions by officials related to inspections. The aim of those bribes is to avoid or reduce the liability that might result from those inspections.

Other common aims of bribes are to obtain official registration (or licensing or certification), either in an expedited fashion or in violation of legislative requirements, or other official actions linked to the recipient's position (eg, a bailiff lifting the arrest on a debtor's account in violation of the legislation on execution proceedings).

There have also been court rulings that describe the aim of illegal payments as 'for general patronage and connivance'. This phrasing could merely reflect poor legal drafting; however, we recommend that companies draw the attention of their employees to such risks when conducting compliance training.

Specifically, based on this court practice, it is possible to conclude that even an unarticulated or vague aim of corruption on the part of the initiator of an illegal payment is sufficient, in the eyes of the courts, to charge a company under article 19.28.

Corporate compliance programmes remain the most promising ground to avoid or decrease liability under article 19.28

The most promising defence available to companies in article 19.28 cases is a robust corporate compliance programme, which should prove the absence of guilt and release the company from liability.

In accordance with article 19.28, a legal entity can be found guilty of a violation only if it had the possibility to observe the law but did not take all possible measures to avoid the violation. The taking of all possible measures by a company encompasses the introduction of an effective and reliable system of compliance controls and measures to prevent corruption.

In accordance with article 13.3 of Federal Law No. 273-FZ on combating corruption of 25 December 2008, companies are obliged to develop and take measures to prevent corruption. The Ministry of Labour and Social Protection has prepared and published a series of documents of an advisory nature on anti-corruption matters, including recommendations on measures for preventing and countering corruption in companies. Those advisory documents contain the Ministry's overview of the standards applicable to corporate compliance programmes, based on Russian, international and foreign experience, as well as practical recommendations on the introduction of corporate compliance programmes.

As practice shows, Russian courts are some way from a unified approach in respect of the assessment of guilt of companies when considering cases under article 19.28; however, there have been some positive developments in this area in the court practice of 2018 to 2019, and the most critical improvements were observed in 2020.

In 2020, only around 30 per cent of the cases did not contain any mention of the guilt of the legal entity as a necessary element of *corpus delicti*, while in previous years these cases represented more than half of all cases.

On the other hand, there has been substantial growth in the number of cases in which courts took note that no measures had been taken to prevent the offence and, when so doing, occasionally referred to article 2.1 of the Administrative Code and article 13.3 of the Law on Combating Corruption. This means that the courts have become increasingly aware of the importance of measures preventing corporate corruption as a basis for discharging liability under article 19.28.

In Russian case law relevant to the application of article 19.28, in 2020 there were still cases with 'strict liability' whereby companies were held liable regardless of whether they were guilty. While examining those cases, the courts would usually indicate that the corruption prevention measures taken by the company concerned cannot bear any impact on its guilt. Further, when examining some cases, the courts would confine themselves to a formal indication to the inadequacy of the measures taken, something that, in their opinion, follows from the mere fact of committing the offence ('the offence would not have been committed had the company taken all possible anti-corruption measures').

In our view, those cases should also be placed into the category of strict liability instances as, in reality, such cases are examined even without enquiring the issue of whether the company concerned is really guilty, and the company incurs liability ipso facto as a result of the offence committed, regardless of the measures taken by the company to prevent the offence. In 2020, the percentage of cases involving strict liability dropped to less than 4 per cent.

Court judgments under article 19.28 make us believe that most companies prosecuted thereunder do not have corporate compliance programmes. This could be the reason why cases like this are rare. Specifically, companies argued that they took all possible measures to prevent corruption in only 12 cases in 2019, but in 2020 this increased to 17. In 2018, we found only nine such cases.

In some cases, in the absence of argument on the part of the company in respect of its corporate compliance programme, the court may prefer to refrain from assessing this issue on its own initiative; however, strictly speaking, courts should conduct this

analysis even where companies keep silent on this issue because guilt is one of the essential elements of an offence under Russian administrative law, which provides for no strict liability.

It is therefore quite difficult to assert that the availability of an effective and well-documented compliance control system can help companies to defend their innocence when indicted under article 19.28 or reduce liability. In the absence of uniform court practice on the matter, the chances of success would depend on the opinion of a particular judge considering the dispute and on credibility of the company's defence; however, it is increasingly clear that the role and efficiency of the defence will grow with each passing year in proportion to the ongoing trends in that sphere.

Majority of fines remain rather low

The majority of bribes in article 19.28 cases are less than 1 million roubles. This limits the fines that could be imposed to a range of 1 million roubles to 20 million roubles.

Courts often reduce the size of the penalty to below the lower limit envisaged by article 19.28. In most cases, this is because of the dire financial condition of the company charged, as well as, sometimes, in observance of the principle of proportionate punishment. We did not find any cases in the period under review in which the court agreed to reduce the fine to below the lower limit owing to anti-corruption measures taken by a company.

Conclusion

We anticipate that in the foreseeable future, more and more companies (and more and more larger companies) will be targeted by Russian law enforcement agencies, for their own illegal acts or for the illegal acts of their counterparties made in their interests.

Such tendencies in law enforcement practice will further increase the importance of the compliance function. The monitoring and control over activities of counterparties, and processes for the selection of such counterparties, will become increasingly important in the context of potential article 19.28 liability. There will be a growth in the importance of meticulous and timely counterparty due diligence and of training counterparties in anti-corruption compliance standards.

Companies should immediately start taking the appropriate measures. Offences committed now will be the subject of investigation and court proceedings in the years to come and will encounter changing conditions in terms of court practice.

Experience shows that in those situations, it is highly desirable for companies not to simply adhere to the letter of the law but to develop and introduce standards exceeding the statutory requirements.

PAUL MELLING
Baker McKenzie

Paul Melling is an English solicitor who has spent his entire professional career working in the countries of the former USSR, having opened Baker McKenzie's Moscow office in January 1989. He has been resident and practising law in Moscow for over 30 years. In addition to being the founding partner of Baker McKenzie Moscow, he also opened his firm's Almaty office in 1995. He is the founder and leader of Baker McKenzie's compliance and investigations group in Moscow. He is also honorary legal adviser to the British Ambassador to Russia and a member of the Advisory Council of the Russo–British Chamber of Commerce.

Paul is known particularly for his work with multinational corporations in the life sciences sector (both pharmaceuticals and medical devices). In *Chambers Europe 2020*, he was ranked as an 'Eminent Practitioner' in the life sciences section and, as far back as 2009, he received the Distinguished Service Award from the Association of International Pharmaceutical Manufacturers for his 'Outstanding Contribution to the Development of the Russian Pharmaceuticals Market'.

ROMAN BUTENKO
Baker McKenzie

Roman Butenko is a senior associate in Baker McKenzie's Moscow office and a criminal advocate admitted to the Moscow city bar. He is experienced in the area of anti-bribery compliance and investigations, criminal law and dispute resolution. Roman has a PhD in law and is a visiting lecturer at the Russian Ministry of Economic Development, as well as at a number of leading Russian universities, where he lectures on anti-corruption compliance matters.

Roman has extensive experience in internal investigations and compliance advisory work across various regions and industries, including healthcare, TMT, energy and mining, and others.

Roman spent around one year in the Washington, DC office of Baker McKenzie, where he advised and assisted clients on various anti-bribery compliance matters. He has also gained the unique multicultural experience of advising and representing clients across Central Asian jurisdictions during his over two-year practice in Almaty, Kazakhstan.

For more than 70 years, Baker McKenzie has been effectively providing global advice for large domestic and multinational clients and for over 30 of those years providing such advice in Russia. The size and global reach of our firm, with its 78 offices in 46 countries, guarantees that know-how is shared among jurisdictions and allows resources from our international network to supplement local office needs. Our lawyers advise clients on criminal and criminal procedure law issues, represent clients and their management before law enforcement authorities and regulators and lead internal investigations in response to allegations of the violations potentially leading to criminal and administrative liability (white-collar crimes). Baker McKenzie was ranked as a leading law firm in Russia for its white-collar crime practice in *The Legal 500 EMEA 2020*.

White Gardens, 10th Floor
9 Lesnaya Street
Moscow 125196
Russia
Tel: +7 495 787 2700
www.bakermckenzie.com

Paul Melling
paul.melling@bakermckenzie.com

Roman Butenko
roman.butenko@bakermckenzie.com

Internal Investigations: Swiss Law Aspects

Juerg Bloch and Philipp Candreia
Niederer Kraft Frey Ltd

IN SUMMARY

Internal investigations have become an increasingly important and integral part of prudent corporate governance in Switzerland. This article provides a brief overview of the key considerations that will allow a Swiss-domiciled company to conduct an effective internal investigation. The topics addressed in this article include typical triggers of an internal investigation, specific questions that must be addressed by the company if an investigation is about to be launched, the impact of secrecy obligations on data collection in Switzerland, the use of specific findings with regard to pending or anticipated court or other official proceedings and questions on cross-border data transfer from Switzerland. We conclude this article by highlighting certain practical recommendations for Swiss companies to prepare for potential future internal investigations.

DISCUSSION POINTS

- Set-up of an internal investigations (governance, scope and work product)
- Conduct of an internal investigation (data collection and review process, e-discovery and employment aspects)
- Particular aspects to be considered with regard to cross-border aspects of investigations (data protection, secrecy obligations and blocking statutes)

REFERENCED IN THIS ARTICLE

- Federal Data Protection Act of 19 June 1992 (status as at 1 March 2019) SR 235.1
- Federal Data Protection and Information Commissioner
- Code of Obligations of 30 March 1922 (status as at 1 January 2022), SR 220
- Financial Markets Supervisory Authority
- Penal Code of 21 December 1937 (status as at 1 January 2022), SR 311.0

Introduction

Over the past decade, internal investigations have become an increasingly important and integral part of prudent corporate governance in Switzerland. While this is particularly true for regulated financial institutions, catalysed especially by US Department of Justice investigations, internal investigations have also become market practice good governance tools for non-regulated entities.

In the wake of tightened national and foreign anti-bribery and corruption laws, law enforcement with draconian penalties (and disgorgements of profits) against corporations and convictions of individuals, internal investigations are regularly initiated in connection with bribery, fraud and other compliance matters.

Triggers for internal investigations

An internal investigation should be initiated in case of (plausible and sufficient) indication of criminal activities affecting, or in connection with, an entity's business. According to recent studies by PwC (2020), 47 per cent of the respondent companies on a global level experienced fraud in the past 24 months, and on average six cases of frauds were reported per company.

In Switzerland (based on a 2018 PwC study), 39 per cent of the respondents (listed and non-listed enterprises) experienced fraud within the past 24 months, with more than 12 per cent stating that they did not know whether their organisation had been a victim of fraud in this period.

If criminal activities primarily affect the enterprise internally (eg, in case of internal fraud, mobbing or sexual harassment allegations), the company is often not interested in initiating a public prosecution. Even if the criminals are outside the company that suffers the damage, the company often does not involve public authorities as it may feel threatened by risks to its reputation.

Companies should consider initiating internal investigations in cases of (alleged) material non-compliance with internal or external rules and policies.

For regulated financial institutions, the threshold for initiating an internal investigation is generally lower than for non-regulated entities. The Swiss Financial Markets Supervisory Authority (FINMA) generally expects financial institutions to investigate significant incidents in appropriate detail and to assess the robustness of internal processes and policies.

Furthermore, FINMA may formally request a financial institution to conduct an internal investigation and produce a report to FINMA as part of its ongoing supervision to ensure that the institution continues to meet its licensing requirements at all times.

FINMA may also directly mandate an investigation, in which case it would typically instruct an independent third party (usually a law firm or an audit firm) to conduct the investigation and to prepare a report to the regulator. The costs of such internal investigation (which can be considerable) must generally be borne by the investigated entity.

Internal investigations may also be triggered by investigations or enquiries of other government or regulatory authorities (seg, tax or competition authorities) to determine the risks for and the defence strategy of the company investigated.

Finally, internal investigations can be a useful tool in a post-M&A situation, in particular to assess potential warranty claims.

Set-up of an internal investigation

Introduction

If an internal investigation is about to be launched, a company must address various questions to make the investigation as efficient and legally robust as possible. The success and robustness of an internal investigation largely depend on the decisions taken at the very beginning of the investigation.

The initial questions to be resolved differ if an investigation is not conducted on a voluntary basis but is imposed by a regulator. The topics discussed here focus on conducting a voluntary investigation. If an investigation is imposed by a regulator, the latter will to a large extent dictate the details of the conduct.

Governance structure

The project governance structure is determined at the very beginning of an internal investigation. It is key for the success of a voluntary internal investigation that, at the top, a steering committee comprising persons with the necessary influence in the company supports and supervises the project.

The steering committee should establish and supervise the project management team, which comprises internal – and, depending on the individual circumstances, external – personnel with adequate knowledge, expertise and independence who closely manage the project on a day-to-day basis. A project office may provide administrative support both to the steering committee and to the project management.

The governance structure must be carefully formalised to provide the best protection for Swiss and foreign legal and work product privilege.

Mandate and scope

Before launching an internal investigation, the project management should be given a clear and unambiguous mandate and task. The mandate should be based on an initial analysis of the issue. The board of directors of the company, as the ultimate supervisory body, is often best-placed to determine the mandate, except in the case of matters with low substantive risks and a small scope and those that do not involve top management.

The mandate should formalise the topic and the goal of the investigation. Accordingly, at the outset of the investigation, the company should prepare a formal document (eg, a resolution of the board of directors, an engagement letter or a memorandum) authorising the investigation and outlining the specific scope of the investigation. Furthermore, resources (personnel and IT) and a budget must be allocated. The mandate should state what the incident triggering the investigation was.

Risk assessment

During an investigation, a company regularly obtains sensitive information about employees, competitors and other third parties. When defining the scope of the mandate, it is therefore paramount that the company is aware of the obligations and risks associated with obtaining certain information (eg, ad hoc publicity obligations) and creating certain work products (eg, production requests by third parties in civil litigation proceedings and criminal investigations).

With regard to the latter, the company must assess to what extent the results and work products of the internal investigation (eg, a final written report or interview records) may have to be disclosed to third parties and how those risks may be mitigated.

Reporting and communication

Clear reporting lines must be established, and a comprehensive reporting system implemented. As a rule, the steering committee should formalise in writing who reports what to whom at what point and in what format.

Periodic reporting is advantageous (eg, in the case of ad hoc publicity obligations of the investigated entity). The reporting concept should also determine when and how matters are escalated internally and a plan for any external communication (the media aspect), including the respective competences, should be set up.

Communication is a necessary part of the immediate measures to be taken after the initiation of an internal investigation as external communication can have a significant influence on public opinion about the company. Proper dealing with the media may help maintain or re-establish public (and particularly investor) confidence in the company.

Work product

At the outset of the investigation, consideration must be made on how the final product of the investigation will be presented. This is often a written report setting out:

- the methodology, process and the available data and information;
- the facts established; and
- conclusions, including proposals to improve, for example, control mechanisms and compliance in general.

A written report may not always be recommendable, in particular with regard to the risk that the work product is (involuntarily) disclosed to a regulator, in civil proceedings or in the course of a criminal investigation. This holds true even if the investigation is conducted by Swiss outside legal counsel as the applicability of Swiss legal privilege to investigation work products has been limited by recent decisions of the Swiss Federal Supreme Court.

If the investigation is conducted in-house, there is no in-house legal privilege under Swiss law. Against this background, there is an increasing tendency to request verbal reporting in a board of directors' meeting, possibly combined with a key findings presentation.

Confidential or disclosed investigation

A decision must be made at the outset of an internal investigation about whether the investigation will be disclosed to employees or whether it should be conducted on a confidential basis. In Switzerland, it is not necessary to obtain approval from employee representatives or similar bodies to conduct an internal investigation. It is also not necessary to inform employees about whom an investigation will be conducted against.

There is no general rule regarding whether an internal investigation should be conducted confidentially or be disclosed to employees (in addition to employees involved). Rather, the best set-up is determined on a case-by-case basis, as well as in light of the scope of the internal investigation and the number of employees involved.

In the case of post-M&A investigations, information from employees may provide the most useful results.

In-house versus external counsel

Internal investigations may either be conducted in-house (eg, by using internal business people, in-house lawyers or internal audit employees) or by independent external investigators. The advantages of having the investigation conducted by external investigators (with substantial support by the investigated company's internal staff) are:

- the absence of conflicts of interest;
- broader market expertise;
- experienced, specifically trained staff; and
- well-established collaboration with related service providers (eg, forensic e-discovery service providers).

In addition, the independence of external investigators is often a key factor for third parties (eg, shareholders, regulators and authorities) to add credibility and reliance to the internal investigation.

When choosing an external investigator, a company should carefully consider whether to task its long-time legal counsel or another outside legal firm. While long-time corporate counsel will be very familiar with the company and could get swiftly up to speed with an internal investigation, which may save time and costs, there is also a risk that a company's long-time counsel (and even more so the company's auditors) lack independence and may become subject to ethical conflicts and divergent incentives.

Conduct of an investigation

Secrecy obligations provided by various Swiss laws and regulations can have an impact on or may hinder internal investigations in Switzerland. Strong secrecy obligations apply to banks, securities firms and certain other financial institutions.

There are also general secrecy provisions regarding business secrets and economic espionage, as well as contractual confidentiality obligations that may oblige a company to secrecy. The respective provisions are set forth in various laws and regulations.

The investigator must ascertain that the data established in the frame of a specific investigation can be used as evidence in court proceedings, if necessary, and must avoid any breach of the prohibitions set forth in the Penal Code (PC) to gather evidence in Switzerland in connection with foreign proceedings (article 271, PC).

Data collection

The company may review its own files and may interview employees if they consent. In cases of severe misconduct, it can prove advantageous to mandate external experts familiar with interview techniques and tactics.

For a review of email correspondence, the rules applicable to electronic discovery must be observed. These rules also apply for a review of, for example, letters addressed to an employee in the files of the company. Further measures include the collection of audio and video material, GPS data analysis or observations by private investigator firms. Such measures are only permitted as long as the personal rights and the health of the employee are not infringed.

For further measures, such as the tapping or recording of telephone conversations, it may be necessary to involve state prosecutors as the company is prohibited from using such far-reaching and delicate measures. The company should be careful not to unnecessarily escalate the data retrieval as, for example, the use of espionage software may render other instruments (eg, termination of the employee) void.

With regard to data collection, contrary to other countries, the current Swiss Data Protection Act also protects the data of legal entities, not only individuals; however, a new data protection act was passed in Parliament in September 2020. Under the new act, which is expected to enter into force on 1 September 2023, only the data of individuals will be protected.

Electronic discovery

As in other jurisdictions, a key part of any internal investigation in Switzerland is the electronic discovery of data. Electronic discovery is mainly governed by guidelines issued by the Federal Data Protection and Information Commissioner (FDPIC)[1] on internet and email supervision by employees (latest version September 2013) and personal data processing in employment (latest version October 2014). In prudentially supervised companies such as banks and insurers, legal obligations may serve as justification for the supervision of secondary data in emails, such as recipients or the time of sending.

1 www.edoeb.admin.ch.

If the company has implemented an internal regulation on the supervision of email and message traffic (which is recommended), the regulation may justify the retrieval of information from emails and messaging services – in particular if the employee has consented to such internal regulation beforehand, for example, as part of his or her employment agreement.

The company in each case must meticulously observe the principle of proportionality in actions taken against employees. Unless there is a strong suspicion of employee misconduct, the company must not supervise the entirety of the behaviour of the employees in question (eg, by installing video cameras supervising the employee all day).

If the company has a clear and present suspicion of abuse, it may review emails specifically concerning a certain employee; however, this does not include emails labelled as private or archived in an electronic folder. If emails are unlabelled or labelled other than 'private', the company may generally assume that they are business-related and may review them.

While a company generally has the right to request and review all business-related data (including emails and text messages), particular issues arise in connection with the use of web-based services, such as WhatsApp, where it is generally not practically possible to gather related data stored on non-Swiss servers.

Employee interviews

As a rule, internal investigations in Switzerland do not require the approval of employee representatives or workers' councils. It is also not necessary to inform employees about pending investigations, in particular if the company's interests in keeping the investigation confidential outweigh the employees' interests; however, it is often advisable in many cases to inform employees beforehand – they often learn about the investigation themselves anyway and usually consent to it, for example, by granting access to emails and documents.

Under Swiss employment law, employees must participate in interviews and provide truthful and complete information. If an employee becomes subject to criminal prosecution, certain limitations to the employee's duty to cooperate may apply; however, there is no uniform opinion in Switzerland on whether the employee can refuse to cooperate (specifically based on the privilege against self-incrimination) or whether self-incriminating statements by the employee made during internal investigations are inadmissible evidence in a (subsequent) criminal governmental investigation.

The Swiss Federal Supreme Court has yet to rule on this question. If an employee participates in an interview, the company may, as a rule, assume that the employee also implicitly consents to the investigation.

It is not entirely clear under Swiss law whether the employee has the right to request attendance of his or her own attorney. Under certain circumstances, however, legal representation can be encouraged to facilitate the conduct of the interview and for the employee to feel more protected and thus more likely to cooperate.

The company generally does not need to provide an attorney for the employee at the company's cost; however, in view of their duty of care towards employees, companies often do provide access to an attorney at the company's cost in the case of investigations triggered by regulators or authorities. In practice, companies regularly pay those fees as a result of directors' and officers' liability insurance coverage.

It is disputed under Swiss law whether the employer must inform the employee about its suspicions prior to holding the interview. Pursuant to the Code of Obligations, the employer may only retrieve data about a specific employee to the extent that the data retrieval is required for proper performance of the employment or to determine the suitability of the employee. The interpretation of this rule is, however, highly disputed in Switzerland.

The company must, furthermore, determine if and to what extent employee interviews should be recorded. If detailed minutes are taken, a court may subsequently find that the employee's value as a witness in court is diminished.

Use of findings

The use of the findings of an investigation in the context of court or other official proceedings depends on the type of proceedings in question. As a general rule, the 'fruit of the poisonous tree' doctrine is not applicable under Swiss law.

In criminal investigations, a court will usually ask whether the evidence could have been obtained legally by the state authorities and whether a balancing of interest (severity of the crime or infringement of personal rights by the obtaining of the evidence) weighs in favour of using the evidence (which is typically the case).

In civil proceedings, evidence obtained by illegal means will only be taken into consideration if the interest in finding the truth clearly prevails.

In administrative proceedings, the rules for criminal proceedings are usually applied.

A company conducting an investigation has a strong interest to obtain evidence through legal means, especially as gathering evidence by other means may expose the company itself to criminal actions.

Data transfer abroad

To the extent that data gathered is transferred abroad, the rules of article 273 of the PC (and other similar secrecy rules), which effectively prohibits the disclosure abroad of non-public third-party information with a sufficient nexus to Switzerland, must be complied with, in particular by appropriately redacting relevant third-party information; however, documents may be transmitted in unredacted form if the third party has consented to the disclosure of its details and if no state interests are involved.

The Federal Data Protection Act prohibits any transfer if, in the country of the recipient, there is no data protection comparable to Swiss data protection. The US data protection regulations are deemed insufficient from the perspective of Swiss data protection law (even in the case of a Privacy Shield certification); however, a transfer may be permitted without consent if it is necessary to enforce claims in court or if there are overarching public interests (pure private interests are not sufficient).

Furthermore, there is a group privilege to transfer data within a group of companies (subject to robust group internal data protection rules and subject to prior notification of the FDPIC). If a cross-border transfer is an issue, the storage and analysis of the data is typically done in Switzerland, and the results are only transmitted abroad in an anonymous manner. As a consequence, the servers used in the investigation should be located on Swiss territory and be accessed from and reviewed in Switzerland.

For investigations initiated by a foreign authority or proceedings in a foreign court, article 271 of the PC must be observed. Acts undertaken in Switzerland for and on behalf of (or for the benefit of) a foreign state that, in Switzerland, would be acts reserved to a public authority are prohibited, unless expressly authorised by the federal government, to avoid circumvention of mutual judicial and administrative assistance procedures.

In this regard, the collection of evidence, even in civil law court proceedings, is considered as an act reserved to state officials under Swiss law (as Switzerland has no concept equivalent to that of US pretrial discovery) and accordingly is subject to the limitations of article 271 of the PC. As article 271 of the PC protects Swiss public authorities, it has no extraterritorial application.

Accordingly, article 271 does not come into play in circumstances where evidence is collected and reviewed outside Switzerland, including, for example, if interviews with Swiss employees are conducted abroad. Consent by the involved persons does not prevent the actions taken in Switzerland from being illegal, and acts prior to the initiation of court proceedings may sometimes be considered illegal.

As a rule, a party in foreign court proceedings may (with certain specific limitations) submit its own documents to support its position in the foreign proceedings; however, it may not file documents compelled by a court order (similar rules apply to third parties being called as witnesses). A third party may only respond to general enquiries.

In connection with internal investigations conducted in Switzerland, article 271 of the PC may become an issue if the investigation is conducted with a view to later providing the work product or documents collected to foreign authorities or courts.

Articles 271 and 273 of the PC do not apply to the company in cases where information is provided through administrative or judicial assistance channels. In particular, in connection with foreign proceedings and investigations, the company should to the extent possible request foreign authorities and courts to seek information through the route of administrative or judicial assistance.

Early preparation highly recommendable

In light of the issues summarised in this article, a Swiss-domiciled company is well advised to prepare early for possible internal investigations. In summary, the following steps are strongly recommended:

- Allocation of competence: the company should establish whether the compliance, legal or risk departments are competent to analyse trigger incidents and determine who should lead an investigation.
- Allocation mechanism for investigation budget: the company needs a mechanism to allocate a budget quickly to the investigation team (costs of internal investigations can be very considerable, especially if non-Swiss lawyers are involved).
- Employee training: ideally a company should build up certain competences (including training) in the relevant departments (which are typically compliance, legal or internal audit). As part of this training, standard proceedings and standard documents (eg, interview forms) can be prepared. Larger companies may consider obtaining forensic software and reviewing their document management systems in the context of their suitability for investigations.
- Employment contracts and regulations: these may be reviewed and adapted to permit the company to send employees on garden leave and to review their emails. The entity's email policy will ideally state that the email account may not be used for private purposes.

- Regulation on email supervision: the company should issue a regulation on email supervision. Among the further documents that can be prepared are regulations concerning document retention and application for Sunday and night work for the project team.

The company should also consider establishing a whistle-blowing policy, which should provide a clear reaction mechanism and protect the whistle-blower.

JUERG BLOCH
Niederer Kraft Frey Ltd

Juerg Bloch is a partner in NKF's litigation department who focuses his practice on advising companies and individuals on corporate internal and regulatory investigations, white-collar crime, crisis management, international mutual legal assistance and compliance matters.

Juerg and his team have represented numerous financial institutions and major corporations as well as their senior management in large-scale cross-border investigations initiated by Swiss and US authorities. In addition, he has conducted comprehensive reviews of corporate compliance programmes and advised organisations on the implementation of best practice in regulatory compliance, anti-corruption and whistle-blower regulations.

Juerg holds a Doctor of Law from University of Fribourg and received an LLM degree from New York University School of Law. He is qualified to practise in Switzerland and New York. He has authored numerous articles within his fields of specialisation and is a frequent speaker at conferences.

Juerg is listed by GIR and *Who's Who Legal* as a 'Future Leader' in investigations for 2019, 2020, 2021 and 2022. In addition, he was recognised by GIR in their '40 under 40' feature in 2020. Sources describe him as an 'exceptionally bright, extremely hard-working attorney, who is always available and 100 per cent dedicated' and 'a technically excellent' lawyer with notable experience in external and internal investigations.

PHILIPP CANDREIA
Niederer Kraft Frey Ltd

Philipp Candreia specialises in complex M&A transactions in various industries with a focus on regulated entities, in particular financial services. He also advises in internal and regulatory investigations and enforcement matters primarily involving large-scale investigations in cross-border compliance matters.

Philipp frequently advises clients on stock exchange and banking regulatory matters and general corporate law, and he assists borrowers and lenders in respect of loan facilities for general corporate purposes and acquisition finance. He also advises clients on shareholding disclosure obligations under Swiss stock exchange regulations and represents clients before the Swiss Financial Markets Supervisory Authority (FINMA) in connection with applications for, and changes to, licences for FINMA-regulated activities.

Philipp graduated from the University of St Gallen (HSG), holds a Doctor of Law from the University of Zurich and received an LLM degree from the University of Cambridge. He is qualified to practise in Switzerland. He is the author of numerous articles within his fields of specialisation and is a frequent speaker at conferences.

NIEDERER KRAFT FREY

Established in 1936, Niederer Kraft Frey (NKF) is a leading Swiss firm with a consistent track record of delivering excellence and innovation in Swiss law. With a strong domestic and international client base, NKF is relied on by the world's best law firms as an experienced, agile and effective partner.

NKF is a full-service law firm with over 100 lawyers advising in 12 languages. We are pragmatic generalists with deep industry knowledge and specialist legal expertise covering the entire spectrum of business, corporate and finance law. We work creatively with each other, our partner firms and our clients to deliver efficient, sustainable solutions in the face of the most complex problems. Quality service is our priority. The focus of our business is the business of our clients.

With offices in the heart of Zurich's banking and financial district, NKF continues to have its finger on the pulse of Swiss business.

Bahnhofstrasse 53
8001 Zurich
Switzerland
Tel: +41 58 800 8000
Fax: +41 58 800 8080
www.nkf.ch

Juerg Bloch
juerg.bloch@nkf.ch

Philipp Candreia
philipp.candreia@nkf.ch

Investigations Involving Third Parties: Practical Considerations for UK Organisations

Michael Zimmern, Alecia Futerman, Joyce Nkini-Iwisi and Kanupriya Jain
Control Risks

IN SUMMARY

Despite being a focus for compliance teams in the United Kingdom for many years, third-party management remains a challenge, with organisations continuing to search for the most effective ways to influence conduct and quickly identify and act on risk. Legislative developments and recent enforcement activity illustrate the increasing expectations placed on organisations around third-party compliance. This article provides practical guidance on approaches to engaging with and monitoring third parties across multiple jurisdictions, including suggestions for overcoming potential roadblocks to investigations.

DISCUSSION POINTS

- Changing landscape of UK law and increasing regulatory risk around third-parties
- Use of due diligence as first line of defence
- Challenges for organisations engaging with third-party agents, intermediaries or partners
- Guidance on approaches to continuous monitoring
- Barriers to conducting and completing third-party reviews
- Consideration of potential investigation outcomes

REFERENCED IN THIS ARTICLE

- UK Ministry of Justice guidance
- *UK Serious Fraud Office v Amec Foster Wheeler Energy Limited*
- *UK Serious Fraud Office v Petrofac Limited*
- *Alstom Transport SA v Alexander Brothers Ltd*
- US DOJ, Evaluation of Corporate Compliance Programs (updated June 2020)

Introduction

Third parties have long been identified as posing a key compliance risk for organisations, with analysis showing that between 1977 and 2022, nearly 90 per cent of all US Foreign Corrupt Practices Act-related enforcement actions involved third-party intermediaries, such as agents, consultants and contractors.[1]

The picture in the United Kingdom is similar, with UK agencies – including the Serious Fraud Office (SFO), the Financial Conduct Authority and the National Crime Agency – repeatedly highlighting the role of third parties in relation to enforcement action taken in the past five years. For example, in 2021 the SFO described the role of third parties, particularly agents, in facilitating the payment of bribes in connection with cases settled in the year:

> *A key feature of the case was the complex and deliberately opaque methods used by these senior executives to pay agents across borders, disguising payments through sub-contractors, creating fake contracts for fictitious services and, in some cases, passing bribes through more than one agent and one country, to disguise their actions.*[2]

The SFO further stated the following:

> *In the course of the investigation, the SFO has identified evidence which demonstrates that FWEL used agents to assist it in obtaining or retaining business, or an advantage in the conduct of business. The SFO alleges that FWEL's employees and directors conspired with others (most notably agents) to make corrupt payments to public officials.*[3]

Beyond bribery and corruption, third parties also feature in relation to compliance topics from supply chain integrity to sanctions compliance, with recent UK legislation such as the Modern Slavery Act of 2015 and the expanded sanctions regime increasing the need for companies to actively manage their third-party relationships.

1 Stanford Law School, Foreign Corrupt Practices Act: Statistics & Analytics.

2 Serious Fraud Office (SFO), 'Serious Fraud Office secures third set of Petrofac bribery convictions' (4 October 2021).

3 SFO, 'SFO enters into £103m DPA with Amec Foster Wheeler Energy Limited' (2 July 2021).

Despite being a fundamental part of business and a focus for compliance teams in the United Kingdom for many years, third-party management remains a challenge, with organisations continuing to search for the most effective ways to influence conduct and quickly identify and act on risk, not only at the point of onboarding but also throughout the life cycle of the relationship.

Third-party compliance

Third-party checks are a key building block of a robust anti-bribery and corruption compliance programme and a baseline expectation of most bribery and corruption standards, for example:

> *a company's third-party management practices are a factor that prosecutors should assess to determine whether a compliance program is in fact able to "detect the particular types of misconduct most likely to occur in a particular corporation's line of business.*[4]

Although some organisations only focus on their third-party compliance programme in response to misconduct, regulatory pressure or stakeholder expectations, most large British organisations with international operations have actively engaged in improving their approach to third-party compliance.

A typical third-party compliance framework will include due diligence processes applied to new third parties during onboarding and existing third parties on a periodic basis.

Due diligence activities may include a review of publicly available corporate information and a search of watch lists and can extend to mapping the corporate structure and ultimate beneficial ownership of the organisation, or the use of human sources to provide their perspective on the reputation and profile of the company, its shareholders and management, and aspects of its operations and supply chain.

These processes follow a structured workflow of planned checks and, in order to be effective, require organisations to establish an accurate view of their third-party population and the nature of their relationships with different third parties.

Effective due diligence programmes are a key part of third-party compliance programmes and can be used to obtain available corporate information that helps organisations to filter out partners with known red flags or a poor track record; however,

4 US Department of Justice (DoJ), 'Evaluation of Corporate Compliance Programs' (June 2020), page 8.

in some instances, there are gaps in the public record, or the available information is conflicting or unclear. Even where the due diligence is clear, it is not only the integrity of the third party, but the substance of the relationship between the organisation and the third party that must be understood in assessing risk.

Potential risks

For organisations to determine whether further steps are proportionate in assessing underlying third-party relationships and investigating concerns, it is necessary to understand how third-party relationships can lead to compliance challenges. The following section summarises three areas where clients often encounter challenges.

Outsourcing risk

In some cases, individuals within an organisation can collude with a third party to facilitate bribery, circumvent company controls or provide distance and deniability in transactions commissioned for the benefit of the organisation.

Examples of ways third-party relationships can be exploited	Control weaknesses associated with these activities
• Use by the third party of commissions, sales incentives or other receipts from the company to pay kickbacks to the ultimate customer • Payments to the third party by the company for fictitious or overvalued goods and services (eg, rental payments or salaries to fictitious individuals) either to pass additional funds to an associate or to create slush funds, enabling the third party to make payments in cash • Using payments presented as charitable contributions or social investments (eg, to schools, hospitals and community projects) as a means of hiding corrupt payments to either the ultimate beneficiaries of the charitable organisations or those involved in the projects • Use of distributors or agents to supply restricted customers or offer commercial terms that would not be permitted by the company • Using suppliers that do not comply with restrictions or regulations that apply to the company (eg, sanctions or child labour)	• Lack of clear pricing and incentive structures, resulting in limited transparency over remuneration calculations • Generous or undefined discount, rebate or commission structures potentially being used by the intermediary to channel kickbacks to customers or disproportionately reward preferred or connected associates • Insufficient or ineffective review processes enabling procurement of services that are hard to measure or value and where the business context is not clear • Lack of identification of the ultimate beneficiary of payments • Lack of visibility over the complete population of third parties, enabling entities to be paid out of petty cash or expenses, or through general codes or retained out of contract, thereby avoiding standard processes and checks

Examples of ways third-party relationships can be exploited	Control weaknesses associated with these activities
• Local third parties engaged to operate as the representatives of the company or to meet operating requirements in the country – these entities may be engaged in licensing, employment or sales activities on behalf of the company, and such structures are necessary to enable operation in some markets but can also be abused by the third party or the parent company, or both	

Weaknesses in internal controls, or a lack of risk awareness within the business, can also allow high-risk entities and interactions to pass onboarding processes and standard transaction approvals. More detailed analysis and review is sometimes required to identify risk.

Use of subcontractors

Even where there have been thorough checks on a prospective third party, there may be a lack of oversight regarding how the third party will fulfil the contract and who will perform the work. If subcontractors or additional entities are involved, due diligence on the immediate supplier may not be sufficient to address:

- the risk of poor-quality work arising from unvetted providers that impacts the overall project delivery, cost and quality; or
- the risk of the subcontractor being used as part of a scheme to conceal the transfer of value from the third party (and ultimately the company).

Common red flags include:

- a recently set-up firm with limited or non-existent reputation or qualifications;
- a low number of employees relative to the work required;
- a lack of evidence of the need for work or why the subcontractor is required; and
- a lack of clarity regarding ownership of the company or links between the third party and the subcontracted entity.

A detailed understanding of the local context is often required when assessing the role of a subcontractor or supporting entity. In some cases, local content rules may require the use of domestic partners, but risks can be magnified where local officials insist on particular companies being engaged or where the population of accredited or qualified entities leaves limited choice for the company.

Attitude to compliance

The mere fact that a supplier or intermediary does not present red flags and passes due diligence checks does not mean the organisation shares the values of the company or a commitment to compliance. Some third parties, particularly smaller organisations, can have less developed compliance practices and may not have relevant staff training, necessary processes or confidential channels for people to report any concerns.

This is not to say all third parties should have the same systems in place, with organisations of different sizes, operating in different markets, likely to require different structures proportionate to their needs and risks. In some cases, it can be difficult for smaller entities to produce the full raft of compliance documentation expected of them, and this can interpreted, sometimes unfairly, as indicating a lack of regard for integrity and compliance.

UK companies operating abroad can also be faced with partner entities that are governed by different local legislation, for example, in relation to the treatment of facilitation payments or the definition of public officials; however, regardless of the details of the compliance framework, it is always important to consider whether the values and ways of doing business of the two entities are aligned.

At the extreme end, some organisations have a very limited regard for compliance, with some local representatives willing to pay bribes or offer lavish gifts and entertainment on behalf of their clients to secure contract awards and obtain licences or permits. Differentiating between an immature compliance programme and an entity that does not take compliance seriously can be difficult to do without more detailed checks.

Where there is potential risk, further work is often required to enable an understanding of how the third party does business and the business context for the relationship, as well as a more detailed review of transactions.

The expectation that organisations will go beyond due diligence where necessary has been explicitly stated. For example, according to the UK Ministry of Justice adequate procedures guidance:

> *In higher risk situations, due diligence may include conducting direct interrogative enquiries, indirect investigations, or general research on proposed associated persons. Appraisal and continued monitoring of recruited or engaged 'associated' persons may also be required, proportionate to the identified risks.*[5]

5 UK Ministry of Justice, 'Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010)' (March 2011), page 28.

This message has subsequently been reinforced by others, including the US Department of Justice, in its 2020 Evaluation of Corporate Compliance Programs best practice guidance:

> *Prosecutors should further assess whether the company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party.*[6]

Ongoing engagement and monitoring

Any additional monitoring should focus on third parties with characteristics that have the greatest potential to cause reputational and financial damage. Such considerations are likely to include an assessment of whether the third party:

- acts as a representative of the company;
- makes payments on behalf of the company;
- engages with public officials;
- operates in markets or activities that are considered to be more risky; or
- has been implicated in internal or external allegations or reports.

We have also observed a growing appetite to conduct proactive as well as retrospective reviews, including transaction-level reviews involving the third-party agent before finalisation of the contract with the end customer.

Given the time, cost and resources required to conduct detailed third-party reviews, it is common for organisations to employ a tiered approach to any additional review steps, enabling the company to focus efforts on a smaller pool of entities that can be refreshed on a rolling basis.

The third-party review programme should be integrated with other compliance processes, including relevant information from due diligence, confidential reporting channels and the findings of other internal reviews, to enable potential red flags identified by other checks to be incorporated into a risk assessment.

Understanding potential wrongdoing often requires access to information held by both the entity or the third party, and the ability to compare the information provided by different sources.

A tiered range of additional compliance steps can include third-party outreach and training, transaction monitoring and detailed entity-level reviews.

---

6 DOJ, 'Evaluation of Corporate Compliance Programs' (June 2020), page 7.

Third-party outreach and training

If prepared in the relevant language and with practical examples, these schemes can help improve the risk awareness and understanding of third-party employees, and can be delivered to multiple entities using common material.

Transaction monitoring

If the data is available on a timely basis, introducing standard tests to map trends and highlight key exceptions and anomalies can be a powerful way of tracking conduct among a group of high-risk third parties. It is useful in those circumstances to segregate the third-party population into groups, for example, by entity type, service or geography.

The most significant limiting factor is often identifying and collecting the required data, with international organisations typically using multiple systems and recording data in different ways. Specific transaction reviews can also be performed.

Where red flags are identified, it is important to develop an approach that enables access to the information necessary to make an informed assessment of the situation.

Detailed entity-level reviews

Detailed entity-level reviews can help to reinforce the commitment of the organisation to ethical conduct. These reviews can either be performed via desktop review or expanded on-site review.

Desktop review	On-site review
• Desktop reviews rely on documents being provided to the review team remotely, which can make it difficult to assess the completeness of the information, although organisations have made great strides with digitisation and remote access • In some cases, remote reviews can make it more challenging to interpret culture and assess the compliance attitude of the third party • Remote reviews may take more time because it can be difficult to compel the partner to cooperate • Desktop reviews can be more cost-effective and can also be consistently delivered by the same team • It is important not to over-rely on email to complete a remote review. More detailed insight and engagement is often obtained through calls and virtual meetings	• Expanded on-site reviews enable greater engagement with the third party and more direct observation of the entity's operations • Observations from the visit can be valuable in forming a view on the credibility and legitimacy of the operations, taking into account factors such as location, office facilities and set-up, and the level of ongoing business activity • It is possible to view the office environment and note whether it contains any compliance material, such as details of confidential reporting hotlines or messages about ethics and integrity • Site visits are preferable if an identified risk needs to be urgently addressed because it is easier to accelerate the flow of information when on-site

Regardless of whether a desktop review or an expanded on-site review is performed, it is important to understand the overall business relationship and history with the third party, test the underlying transactions to inform the focus of the review and carry out an appropriate level of testing.

Any financial data should be clean and reconciled at the outset. Data analysis can then be used to identify anomalies or inconsistencies and to apply standard sample selection methodologies to select an initial risk-based sample for review. Such standard tests can consider high-risk expenditure categories (eg, entertainment) along with tests such as round-sum or high-value payments, transactions recorded close to quarter ends, high-value discounts or transaction references to state-owned enterprises or politically exposed persons.

Any potential red flags should be considered with all available documentation, including relevant internal company correspondence and financial records and explanations sought from management.

Practical challenges to consider

The tone of engagement with the third party is a key part of any review. Although a successful review depends on cooperation, it is also a test of the dynamics of the business relationship. If the review feels like an investigation, it is likely the third party will become defensive and resist cooperation unless it is under significant commercial pressure.

Regardless of the approach, it is unlikely the company will be able to access the full gamut of information relating to the third party that would usually be available in an internal investigation. For example, internal emails and electronic communications at the third party or financial information and documents involving transactions that do not relate directly to the company are usually not available. It is therefore important to engage with the third party in a way that increases the prospects of accessing the maximum amount of relevant information.

A key part of the process, and a critical step in engagement, is facilitating a proper kick-off meeting between all those involved, setting out the aims and objectives of the review, providing an overview of the programme and identifying individuals who can be contacted with questions or concerns.

While the process should feel collaborative, it is important to recognise that the consequences of the review can be significant, so the company and the review team must find the right balance between establishing an effective working relationship and ensuring the importance of the process is appreciated. In practice, the best engagement often happens when the company is prepared to state clearly how serious it is about compliance in general, particularly with regard to its third-party review programme.

Ultimately, if the company cannot reach an understanding where the third party is willing to engage with the review, it is important that the company be willing to consider the implications, recognising the third party is likely to be considered high risk. Some of the best examples of engagement have been when the company has stopped new business with the third party pending results or has made clear the future relationship is contingent on a successful review.

Data access and cooperation

One of the key barriers our clients face is in having the required contractual terms – particularly audit rights and, where necessary, non-disclosure agreements – in place that are acceptable to all parties. While these requirements can often cause delays, they are not usually sufficient to prevent a review from taking place if the right commercial relationship exists.

Even where the appropriate contractual provisions are in place, there are often challenges in accessing information for the review. For example, the third party may have confidentiality considerations that restrict sharing information relating to general operations and that can limit the potential of the review to assess activities such as general business development, including hospitality and entertainment.

Organisations can also seek to use data protection and privacy rules to protect relevant information that may be desired as part of the review. There are also third parties in some countries that can coordinate and share information in an attempt to delay or obfuscate the review. It is therefore important for the company to have anticipated those arguments and reached an agreed internal position on what level of information sharing they are prepared to accept from the third party.

In some countries, staff at the third party engage more openly and extensively with individuals from the same country. Beyond shared language, which is fundamental, having a team familiar with local ways of doing business, business etiquette and business regulations is an important consideration for delivering a successful review.

There can also be difficulties in finding where a third party operates. In the fashion industry, where companies take advantage of cheap labour across South Asia, clothing factories do not always have a proper, published address.

Ultimately, some third parties choose to adopt consistent delaying tactics or simply refuse to cooperate. Failure to engage with the third-party review process should be viewed as a significant red flag, and the company should consider whether ongoing business activity should be paused until further notice.

Concluding the review

For any third-party review to be effective, it is important to act on the results. Given the limitations in data, decisions often need to be made without certainty. Being in possession of potentially relevant but incomplete information is a difficult situation for compliance teams, where any decision not to act may be subject to future review and challenge.[7]

It is therefore important for any decisions to be well documented and for there to be work done to ensure the decision is implemented on the ground. For example, there have been cases where relationships with an entity have been formally discontinued (eg, a contract has not been renewed) but they continue to be used.

Regardless of the outcome, it is important that any review findings be fed back into existing compliance systems to enable the refinement of processes, controls and ongoing monitoring systems, and updates to training and guidance for the business.

In some cases, it may be appropriate to work collaboratively with the third party to support improvement in its compliance processes and develop new information sharing or monitoring solutions; however, in other cases, the company may decide to take more significant action.

Any decisions about changing the third-party relationship should consider the practical aspects of implementation, including the contractual relationship between the parties and the potential impact on the local operating environment. There is a risk that any decision to terminate a relationship owing to concerns about misconduct or corrupt activity by the third party may be subject to legal challenge for breach of contract, failure to pay for goods or services, or loss of profits.[8]

In some cases, third-party relationships that have been initiated to capitalise on the political or community connections of the third party can be difficult to terminate without the risk of retaliation or disruption. It is essential not only to document the decision but also to take time to consider how best to communicate and structure any disengagement.

---

7 For example, see paragraph 13 of the statement of facts released in connection with the deferred prosecution agreement between the UK SFO and Amec Foster Wheeler Energy Limited.

8 See *Alstom Transport SA v Alexander Brothers Ltd*, for example, in relation to *Alexander Brothers Limited (Hong Kong SAR) v Alstom Transport SA and Alstom Network UK Limited* [2020] EWHC 1585 (Comm).

MICHAEL ZIMMERN
Control Risks

Michael Zimmern leads the forensics practice for Control Risks in Europe, the Middle East and Africa. As a qualified accountant with more than 15 years of experience helping organisations respond to regulatory, reputational and financial risks, Michael supports clients with cross-border investigation and compliance matters and has worked alongside governments, regulators and enforcement agencies.

Michael has led investigations into a wide range of allegations, including fraud, bribery, unethical conduct, information leaks, discrimination and human rights abuse. He routinely works with lawyers and other advisers in supporting clients respond to these events. Michael has also led the design and implementation of fraud, bribery and corruption compliance frameworks and the development and delivery of effective compliance monitoring programmes for organisations and their partners.

Michael has worked across the United Kingdom, Europe, the Middle East, Russia, India and Africa and has extensive experience helping clients manage integrity risks in emerging markets. He is a member of the Institute of Chartered Accountants in England and Wales.

ALECIA FUTERMAN
Control Risks

Alecia Futerman is a forensic accountant and associate director in Control Risks' investigations practice covering Europe, the Middle East and Africa. Based in London, Alecia has more than seven years' experience advising and assuring clients across a broad range of geographies and sectors.

Alecia specialises in supporting global organisations with their third-party management risk, specifically with regards to fraud, bribery and corruption and compliance management. She has worked on the ground in Africa, Asia, South America, the Caribbean, Europe and the Middle East, working alongside regulators, law enforcement, external legal counsel and internal investigation and compliance teams.

Alecia led the project management and delivery of compliance reviews for a global sports federation, spanning 30 countries across five continents. She is also responsible for the third-party review programme across Europe, the Middle East and Asia of another of our clients, a global technology company.

Before joining Control Risks, she trained as an auditor at a Big Four accounting firm. Alecia is a member of the Institute of Chartered Accountants in Scotland and is a certified fraud examiner.

JOYCE NKINI-IWISI
Control Risks

Joyce Nkini-Iwisi is a principal who leads Control Risks' forensics practice in Africa. She has a decade of combined experience in forensic investigations, auditing and strategy management.

Joyce specialises in assisting clients with proactive and reactive solutions in the form of forensic investigations and fraud risk management advisory. She works with clients in various industries, including financial institutions, government regulators and state-owned entities, non-government organisations, and mining and technology companies.

Prior to joining Control Risks, Joyce worked for two of the Big Four audit firms in East and South Africa and headed the forensics division of one of South Africa's oldest law firms. She has experience servicing clients across Africa, Europe and Asia and was recognised as one of 'Top 50 Women in Management' at the 2019 WIMA Awards. She is fluent in English and Swahili and is a member of the Association of Certified Fraud Examiners, the Institute of Commercial Forensic Practitioners and the Ethics Institute.

KANUPRIYA JAIN
Control Risks

Kanupriya Jain is a director in Control Risks' investigations practice in the Middle East and North Africa, who is based in Dubai. She has investigated numerous financial and non-financial cases related to corruption, financial statement fraud, revenue sharing and quantification of costs in the Middle East and South Asia regions. She has led proactive fraud risk assessments and trained C-suite client representatives on anti-fraud and corruption.

Kanupriya has led large cross-border investigations between the United Arab Emirates, the United Kingdom, India and the United States over allegations of earnings mismanagement, misappropriation of assets, theft of cash, bribery and corruption, and fraud. She has led proactive and reactive corruption and internal controls reviews, including advising clients on robust policies, procedures and compliance frameworks, and she has also designed fraud and corruption training programmes for clients.

Kanupriya is a chartered accountant with a bachelor's degree in law and is a member of the Association of Certified Fraud Examiners, the Institute of Internal Auditors (UAE) and the Indian Business Professional Council.

Control Risks is a specialist risk consultancy that helps create secure, compliant and resilient organisations. Control Risks partners with law firms and in-house counsel on domestic and multinational engagements, providing unparalleled global expertise, local insight and technology solutions.

Our teams draw on a diverse group of forensic accountants, data experts, fraud examiners, former law enforcement agents, global risk analysts and business intelligence experts to provide investigation and compliance services. A cornerstone of our investigative and consulting expertise, our technology resources are used to identify, aggregate, analyse and report across the complex data sources that are critical to understanding our clients' issues.

Cottons Centre
Cottons Lane
London SE1 2QG
United Kingdom
Tel: +44 20 7970 2100
www.controlrisks.com

Michael Zimmern
michael.zimmern@controlrisks.com

Alecia Futerman
alecia.futerman@controlrisks.com

Joyce Nkini-Iwisi
joyce.nkini-iwisi@controlrisks.com

Kanupriya Jain
kanupriya.jain@controlrisks.com

As well as daily news, GIR curates a range of comprehensive regional reviews. This volume contains insight and thought leadership from 28 pre-eminent practitioners in Europe, the Middle East and Africa. Inside you will find chapters on France, Italy, Romania, Russia, Switzerland, Central Europe, the United Kingdom, and the Gulf Cooperation Council region, and overviews on, among other things anti-money laundering.

Visit globalinvestigationsreview.com
Follow @GIRalerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-869-7