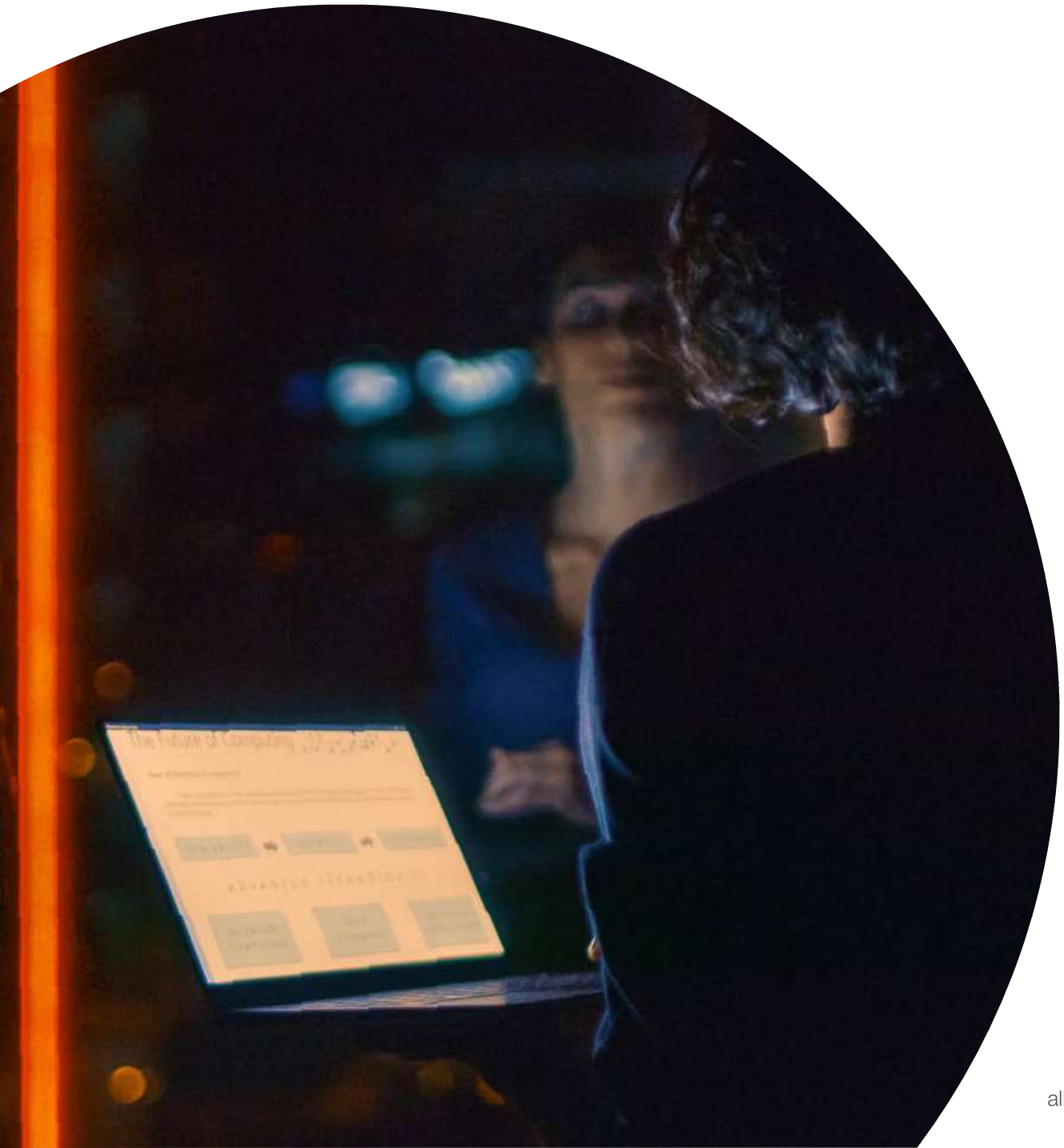
ALLEN & OVERY

Cross-Border White Collar Crime and Investigations Review

2023



allenovery.com

Contents

Introduction

Investigations and financial crime lawyers at large multinational companies faced a plethora of financial crime and investigations developments over the past 12 months, not least the wave of sanctions against Russia. In addition, the economic downturn, stretched compliance resources, and stressed supply chains have increased the risk of misconduct.

In-house Counsel and Heads of Risk will need a laser focus on higher risk areas to mitigate the impact of issues that arise, especially given the increased expectations on corporate behaviour, from a wider range of stakeholders, on issues such as human rights and the environment.

The Allen & Overy Cross-Border White Collar Crime and Investigations Review analyses the latest developments, and highlights the most significant current and emerging issues that white collar crime and investigations in-house counsel should prioritise in 2023.

Looking ahead – Managing key challenges in 2023

We asked our global white collar crime team for their views on key challenges in 2023 for in-house investigations teams and white collar crime lawyers, and how to manage the associated risks.

Be alive to supply chain pressures leading to misconduct

The Russian invasion of Ukraine, and post-pandemic pressures, have led to increased pressure on supply chains. Business pressure to find solutions can inadvertently lead to behaviours that fall foul of laws on bribery and corruption, financial sanctions, terrorism financing (eg for making payment to groups for safe passage of goods in certain territories). Enhanced expectations and, in some countries, specific supply chain due diligence laws mean that such misconduct is less likely to go unnoticed.

How you should respond – make sure that commercial knowledge on pressure points is shared with those who have responsibility for providing risk-based training and guidance on policies and procedures. To mitigate those risks, identify areas/personnel of higher risk based on current events, geographies, and check the local controls and oversight of those controls. Some compliance functions have been stretched due to diversion of resource to sanctions related matters and budgetary constraints. Check that those who remain have the necessary skills and expertise, and time, to adequately support effective compliance. Both the U.S. Department of Justice and the UK Serious Fraud Office are increasingly focusing on resourcing and capability of the compliance function when evaluating a corporate compliance programme.

Understand evolving expectations on corporate accountability on environmental and human rights issues

Expect increased scrutiny of corporate behaviour. Higher standards and expectations on corporate accountability have manifested in different ways across the globe. The direction of travel is firmly towards increased scrutiny of corporate behaviour regarding the environment, people working in, and impacted by, all parts of a company's value chain (including third party suppliers) and employees. In addition, pressure is being exerted by a broader range of stakeholders. Activist shareholders, employees, employees of third party suppliers, local communities and others are using both litigation and reputational levers to hold companies to account for environmental harms and human rights violations. Belgium is likely to be the first European country to introduce a criminal offence of ecocide. The French courts have been upholding unprecedented indictments against companies for aiding and abetting war crimes and crimes against humanity. 2023 will be marked by the development of a wide array of new sustainability obligations for companies operating in the EU.

How you should respond – Prevention is the best medicine so companies should check that compliance and whistleblowing procedures are working as intended – the ongoing implementation of the EU Whistleblowing Directive means that this is an area of focus for many EU Member States. If misconduct is suspected, any internal investigation should be carefully structured to take into account the very real risk of follow-on civil or criminal litigation and regulatory action. Many whistleblowers that communicate with government regulators have first raised concerns internally and not felt their concerns have been adequately addressed. A measured and proportionate whistleblowing response and internal investigations programme may help identify and stop misconduct before external stakeholders are aware.

Don’t take your eye off intermediaries

The use of intermediaries remains a high corruption risk. Almost all FCPA and other corruption cases involve the use of third parties or intermediaries to make corrupt payments. The true purpose of the payments is invariably disguised, such as in improper mark ups, poorly defined “service fees,” or other schemes designed to evade a company’s internal controls. Bribery and corruption remain high on many existing enforcement authorities’ agendas and those of new ones, eg the new Australian Anti-Corruption Commission.

How you should respond – Companies must ensure that their policies and procedures around the hiring of, and commercial terms with, business partners are properly implemented and reviewed on a regular basis to reflect the business as it evolves. Commercial pressures should not be allowed to trump adequate due diligence. Compliance and finance functions need to be properly resourced with staff with the right level of experience and seniority. Not only will this help prevent misconduct, but it will also be a mitigating factor should there be any enforcement action. Data analytics offer insights to drive compliance programmes, and authorities’ expectations in this regard are increasing. Compliance teams should consider whether they use data effectively to: (i) save time and cost; and (ii) inform the design, implementation and effectiveness of compliance programmes.

Ensure corporate culture supports effective compliance, even during an economic downturn

Expect continued scrutiny of how corporate culture and compliance interact. Recent enforcement suggests that merely having policies and procedures in place, even if externally certified, will not necessarily be adequate either to prevent financial crime in an organisation or to provide an ‘adequate procedures’ defence for a company faced with prosecution under English law ‘failure to prevent’ type offences relating to bribery and tax evasion. How the policies and procedures are embedded in an organisation is critical to making them effective. At a time of budget constraints, eg on legal and compliance for many businesses, we still expect to see continued scrutiny by authorities on “tone from the top” and the “tone from the middle”.

How you should respond – How an organisation responds to issues that arise is seen as one of the litmus tests for the culture of an organisation. The implementation of the EU Whistleblower directive across many EU Member States highlights the importance of companies having fit for purpose whistleblowing programmes. The identification of incidents through a proper compliance and whistleblower programme, a prompt and objective investigation, and appropriate and timely remediation not only limits damage for the company but may also be viewed positively by the authorities if the conduct comes to their attention.

Navigate conflicting laws driven by national security and geopolitics

Expect increasing global geopolitical tensions to ensnare more companies. The dynamics of geopolitics and national security concerns mean that businesses can increasingly end up as pawns, often being stuck between conflicting requirements that require delicate navigation. For example:

- The war in Ukraine has led to a surge in sanctions measures relating to Russia, which apply to businesses in all sectors.
- China's data laws add substantial complexity to the cross-border transfer of documents and evidence for investigations, particularly in the context of requests from foreign government authorities, and also for internal investigations.

How you should respond – Companies will need to consider the commercial, legal and enforcement context in order to adopt a sensible path through these national security driven and often conflicting requirements. Make sure that the reasons for internal decisions are properly documented. Where appropriate, maintain an open dialogue with the authorities if the company is unable to comply with a request or order due to conflicting requirements. It can sometimes be possible to negotiate a path forward that avoids direct conflict.

Manage the risk of unsanctioned communication channels for business purposes

The unauthorised use of unmonitored personal devices and encrypted communication applications is widespread, and poses significant enforcement risk, particularly to those in regulated sectors. It also impairs the ability of internal investigators to access and uncover facts quickly should an allegation of misconduct arise. The U.S. Department of Justice is expected to issue new guidance in 2023 in this area for all companies, not just those that operate in highly regulated sectors.

How you should respond – GCs and Heads of Risk must ensure that employment policies and agreements are fit for purpose, and actively policed. One approach is for policies to make clear that personal devices cannot be used for business purposes in any circumstances, and then to reiterate this message in the regular compliance training and communication programme. Privacy and employment laws can pose additional challenges to consider if access to a personal device becomes necessary. A common practice is developing to retain pool counsel or independent counsel for individual employees to review and identify responsive correspondence from an employee's personal device. Obtaining consent to access a personal device, particularly during the throes of an investigation, can create tensions and test your policies and employment agreements.

Investigate how technology can help to quickly and effectively review data to pinpoint key communications during an investigation. Using technology to do the heavy lifting at the document review stage often saves costs in the longer term and narrows the scope of manual review needed.

Be alive to the pinch points on privilege

Expect more pushback when claiming legal privilege. This is not new for 2023, but it remains a challenge in many investigations. There is often a tension between an authority's expectations of cooperation, and rules on legal professional privilege.

How you should respond – In-house counsel are advised to continue to consider carefully how to manage issues of privilege and cooperation, perhaps adopting a tiered approach with "crown jewel" privilege claims (for example, communications with external lawyers) and other privilege claims which it may be less uncomfortable about waiving (for example, notes of interviews with some employees). Any decision to waive privilege must be informed by a strategy to minimise the wider impact of any waiver as well as an analysis of the possible use that an authority may make of the material, including possible onward transmission by the authority to a third party. Additionally, take care to consider privilege laws in the different countries in which you operate and minimise the likelihood of inadvertent waiver by engaging in best practices when conducting internal investigations, for example.

Look after your (and others') data

Expect cybersecurity to remain a priority. Risk has increased due to the Russian invasion of Ukraine and the post-pandemic economic environment. Key threats include:

- malicious cyber actors targeting internet-facing systems, such as email servers and virtual private networks (**VPNs**) with newly disclosed vulnerabilities
- a 300%[1] increase in ransomware attacks since 2019, with the most common entry points being Remote Desktop Protocols (**RDP**) ports as well as unpatched software, hardware or VPNs
- denial of services attacks.

Cybersecurity remains a favourite on many authorities' compliance and enforcement agendas.

How you should respond – Invest in strong defences and experienced personnel while implementing robust processes and procedures so that a business stands ready to react to, respond to and remediate any incidents that occur in a timely fashion and in a manner that considers stakeholder concerns, reporting obligations, and any potential liability. Board engagement is vital, so it should receive regular reporting on cyber risks. Read our blog on considerations for boards.

1 UK FCA Cyber Coordination Group Insights published 8 December 2022.

Expect more investigations to be investigated

When the outcome of an employee misconduct investigation goes against an individual, or a regulator is a stakeholder, the spotlight can turn onto the investigator. Were they independent? Was there a conflict or perceived conflict? Did the investigator have the necessary skill-set to understand the nuances of a particular allegation? Was there institutional bias? What experience did the investigator have in running hybrid, multi disciplinary or multi-jurisdictional investigations? Did the investigator have the necessary time and resources to dedicate to the process? If there are shortcomings in any of these areas, it can lead to the need for a second, independent, external investigation, adding delay and cost.

How you should respond – This can be avoided if time and thought are invested at the outset, when triaging and 'scoping out' investigations, to identify those cases that are, whether optically or practically, more appropriate to be outsourced. For example, if the investigation involves a senior executive with a high profile, outsourcing may help avoid questions of independence. Another example is where the investigation involves serious allegations of sexual or racial harassment and it is felt that the available investigators do not have the appropriate skill set for the investigation. The key point is that these factors need to be taken into account at the outset.

Balance the costs and benefits of self-reporting and cooperation

In-house counsel can face tough decisions on whether and how to self-report and/or cooperate with authorities. Some authorities have a much more active enforcement record than others. The benefits and drawbacks of cooperation vary by jurisdiction. There have been substantial discounts on fines for companies that have not self-reported but pleaded guilty before conviction, thus avoiding a trial.

How you should respond – A decision to cooperate must take into account the time and cost of doing so, and the potential reputational and financial upside, including a potential discount on a fine. This should be compared with what might happen if the business takes a more passive stance.

Our lawyers have strength and depth in many geographical areas and are used to helping our clients navigate all these issues to reach effective and practical solutions. If you would like to discuss any of the issues arising in this publication with our team, please contact amy.edwards@allenovery.com.

Overview of key developments by jurisdiction

Australia

There were high levels of regulatory and enforcement activity in Australia in 2022. The regulatory landscape has continued to experience significant shifts as the economy encounters greater inflation, geo-political tensions, increasing environmental concerns and a growing number of cybersecurity threats. The Australian Securities and Investments Commission (**ASIC**), Australia's financial services regulator, departed from its much-publicised and controversial "why not litigate" approach in favour of an approach that prioritises promoting Australia's economic recovery from the pandemic and the inflationary pressures that are currently being experienced.

With the victory of the Anthony Albanese-led Labor Party over the conservative incumbent government led by now former Prime Minister Scott Morrison in the May 2022 federal election, a steady stream of new legislation has started making its way through federal parliament. Several of these bills will impact white collar crime and investigations, with more reform to come, including in relation to data protection, money laundering and terrorism financing, and corruption.

At the end of 2022, a bill was passed providing for the creation of a National Anti-Corruption Commission, likely mid-way through 2023. It is likely to result in high-profile investigations in the years ahead.

Belgium

Regulatory and criminal enforcement in Belgium remains robust, with a significant uptick in the investigation and prosecution of corruption, environmental pollution, social fraud and human trafficking. Authorities are in particular focusing on the chemical, construction and transportation sectors.

We expect this trend to continue and intensify in light of: (i) increased regulation such as the development of a Business and Human Rights framework and the expected introduction of ecocide as a self-standing criminal offence under the new Belgian Criminal Code; (ii) compliance, in the broadest sense of the word, becoming a focal point for businesses in any sector; and (iii) increased whistleblowing disclosures, driven by the very recent transposition of the EU Whistleblowing Directive.

Financial crime remains high on the cross-border enforcement agenda, and will only gain in importance due to the rapidly increasing caseload of the European Public Prosecutors Office (**EPPO**), increased enforcement activities by financial market regulators and antitrust authorities and recent calls for EU Member States to enforce the myriad of sanctions imposed in response to Russia's invasion of Ukraine.

Mainland China

China's data laws have added substantial complexity to the cross-border transfer of documents and evidence for investigations, particularly in the context of requests from foreign government authorities, and for internal investigations. This will impact how a company can respond to direct requests from non-Chinese authorities in any investigation concerning China-based conduct. Data enforcement activity is also increasing rapidly, and it has been confirmed that foreign-registered entities are captured squarely by the PRC data regime, if processing activities under their direction are carried out in China.

A dip in ABAC enforcement activity against companies in 2022, due to competing governmental priorities (notably Covid), is expected to be temporary, with the government regularly restating its commitment to combat both active and passive bribery.

China's approach to the regulation of non-fungible tokens (**NFTs**) is evolving, and it is expected that regulation will include ensuring that NFTs are not commoditised, in line with China's approach to cryptocurrencies.

France

France remains a key player in white collar enforcement in Europe. As with previous years, the fight against money laundering, tax evasion and corrupt practices remains an enforcement priority, in particular for the National Financial Prosecutor's Office (**PNF**). Corporate responsibility for human rights violations has also been a major enforcement and investigations theme this year with the *Cour de Cassation* (the French Supreme Court) and the Paris Court of Appeal upholding unprecedented indictments against corporates for aiding and abetting war crimes and crimes against humanity. There has also been an ever growing number of French style Deferred Prosecution Agreements (*Convention Judiciaire d'Intérêt Public* (**CJIP**)).

Hong Kong SAR, China

The new Head of Enforcement for the Securities and Futures Commission (**SFC**) may in due course herald a change in regulatory direction and enforcement policy in Hong Kong. Whether or not that occurs, the SFC continues to drive change to better regulate the financial markets. A new consultation proposes changes that would permit the SFC to apply for remedial and other court orders on the basis of disciplinary action rather than breach of certain laws, while the SFC continues to advocate for, and seek to expand its regulatory oversight of, the cryptocurrency sector. Meanwhile, proposed legislative reforms address weaknesses in existing cybersecurity laws and strengthen sanctions.

Germany

Prosecution authorities, as well as criminal courts, continue to investigate the cum/ex complex, which has led to further indictments and convictions in 2022. A significant number of banks and audit firms have been raided in connection with these investigations. We expect to see more in 2023.

The criminal trial against the former CEO of Wirecard and other former senior Wirecard managers regarding allegations of fraud, balance sheet manipulation and other offences commenced before the Munich Regional Court in December 2022. The criminal trial regarding the Wirecard case will likely continue throughout 2023.

The Supply Chain Due Diligence Act came into force on 1 January 2023, and we anticipate the first regulatory enquiries into compliance with the new law. The German legislature is expected to pass the Whistleblower Protection Act early in 2023, meaning that the new law would come into force towards the end of Q1/2023.

Netherlands

The past year has seen a vast increase in attention paid to sanctions legislation due to the ongoing war in Ukraine. Investigations into non-compliance with Anti-Money Laundering regulations also remain a high priority for Dutch enforcement authorities. In addition, the Dutch Public Prosecution Service (DPPS) continues to focus on the prosecution of individuals, in cases where a legal entity enters a settlement with the DPPS. We expect increased scrutiny of tax integrity, cybercrime and business responsibility for human rights in 2023.

South Africa

The risk of the Financial Action Task Force (**FATF**) greylisting looms large over recent South African reforms, as do the ongoing consequences of "state capture". The four-year-long Judicial Commission of Enquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector including Organs of State (**Zondo Commission**) has submitted its final report to the President. The Presidency, Parliament, law enforcement and regulators have shifted to pursuing criminal prosecutions and administrative penalties against offenders, recovering funds and considering necessary legislative and institutional reforms. High profile arrests and settlement agreements relating to state capture and asset freezing related to corporate accounting and reporting fraud have dominated the latter part of 2022. We anticipate that 2023 is likely to see similar arrests, extensive litigation and a raft of legislative reform focused on preventing money-laundering and regulating public procurement. State capture investigations have prompted increasing cooperation between law enforcement and regulatory agencies which has extended to using relatively powerful anti-money laundering, tax evasion and exchange control remedies to combat corporate fraud as well as environmental and cyber-crimes.

United Arab Emirates

2022 was another busy year for the UAE as it sought to further develop its regulatory framework. The UAE continued with significant regulatory development and expansion, including in the areas of anti-money laundering/counter-terrorist financing compliance, whistleblowing, data protection and virtual assets. These developments continue to have implications for both the UAE's onshore jurisdiction and its offshore jurisdictions, including the Dubai International Financial Centre (the **DIFC**) and the Abu Dhabi Global Market (**ADGM**).

We expect to see the UAE authorities place a greater focus on monitoring and enforcing compliance with new and existing regimes in the year ahead. Businesses should therefore take prompt and proactive steps to ensure they are compliant with all regimes applicable to them so that monitoring and enforcement risks on the horizon can be appropriately managed and mitigated.

United Kingdom

The Russian invasion of Ukraine hastened legislative reform aimed at stemming the flow of 'dirty money' in the UK and aiding the enforcement of financial sanctions. Not so hasty is a new 'failure to prevent' economic crime offence, which is still not on the statute books. Supporters of reform will have been pleased with the UK Law Commission's July 2022 report which stated that there is now a 'consensus' on the need for reform of English law on corporate criminal liability, but less pleased that the government has still not decided which, if any, of the Commission's various options for reform to adopt.

The FCA had a busy year in 2022, announcing a number of significant enforcements concerning market misconduct and financial crime, including decisions concerning firms' failure to prevent bribery and corruption. Meanwhile, the SFO was very publicly criticised for multiple disclosure failings which led to high profile acquittals of individuals in large fraud and corruption cases. It was not all bad news for the SFO though, with its largest fine levied against a mining and commodities company for bribery. A new head of the SFO will be appointed in 2023.

The cost of living crisis, stretched compliance resources, and stressed supply chains are an ideal breeding ground for misconduct. Companies should double down on fostering a culture of compliance, and not turn a blind eye to the increasing use by employees of unauthorised encrypted messaging platforms for doing business.

United States

With the implementation of new laws and polices focusing extensively on corporate compliance, companies will have to participate in a more careful consideration of their regulatory obligations. Pivotal to this consideration will be companies' ability to effectively spot issues and address potential compliance failures through internal investigations and effective compliance programming. This enhanced focus on corporate compliance is evidenced by the Biden Administration's commitment to increased enforcement efforts both in civil and criminal enforcement. The U.S. Department of Justice (**DOJ**), the Securities and Exchange Commission (**SEC**), and the Commodity Futures Trading Commission (**CFTC**), among other regulatory agencies, have all shown signs of a more zealous enforcement approach, implementing new policies, expanding corporate disclosure requirements, and allocating more resources to enforcement departments. Crypto-assets, insider trading, sanctions, and record keeping are all prominent areas of focus.

Australia

2022 saw another year of high levels of regulatory and enforcement activity in Australia. The regulatory landscape has continued to experience significant shifts as the economy encounters greater inflation, geo-political tensions, increasing environmental concerns and a growing number of cybersecurity threats. The Australian Securities and Investments Commission (**ASIC**), Australia's financial services regulator, departed from its much-publicised and controversial "why not litigate" approach in favour of an approach that prioritises promoting Australia's economic recovery from the COVID-19 pandemic and the inflationary pressures that are currently being experienced.

With the victory of the Anthony Albanese-led Labor Party over the conservative incumbent government led by now former Prime Minister Scott Morrison in the May 2022 federal election, a steady stream of new legislation has started making its way through federal parliament. Several of these bills will impact white collar crime and investigations, with more reform to come, including in relation to data protection, money laundering and terrorism financing, and corruption.

At the end of 2022, a bill was passed providing for the creation of a National Anti-Corruption Commission, likely mid-way through 2023. It is likely to result in high-profile investigations in the years ahead.

Investigations trends/developments

A move away from ASIC's 'why not litigate' approach

In late 2021, ASIC updated its guidance on its approach to enforcement and published its response to the Australian Government's 'Statement of Expectations', which outlines how the Government expects ASIC will achieve its objectives, carry out its functions and exercise its powers.
These publications evidence ASIC's move away from a 'why not litigate' approach in recent years to a 'lighter more impactful' approach to regulation that identifies and pursues opportunities to contribute to the Government's economic goals, including supporting Australia's economic recovery from the pandemic. ASIC states that it intends to adopt the full suite of its regulatory tools and to do so in a targeted and proportionate way and will decide what cases to pursue through the lens of whether they are going to make a difference. The move away from the 'why not litigate' approach has prompted criticism of ASIC, to which it has responded by noting that ASIC is an active and focused law enforcement agency and is probably the busiest litigator in the Commonwealth. In the period between January and June 2022, 60 investigations were commenced with 148 investigations ongoing. Further, seven civil penalty proceedings were commenced in this period with 40 civil penalty cases still currently before the Courts.

ASIC's targets sustainability, technology risks and product design

The ASIC August 2022 Corporate Plan[2] reveals its strategic priorities for the next four years. These include:

– **Sustainable finance and 'greenwashing'** – to supervise and enforce governance, transparency and disclosure standards in relation to sustainable finance. ASIC is actively monitoring the market for potential greenwashing and has taken enforcement against companies, including a listed energy company.

– **Technology risks** – to promote good cyber risk and resilience practices and address digital misconduct such as scams. ASIC successfully brought Australia's first test case against a company for failing to have adequate cybersecurity systems and processes in place, in breach of its Australian Financial Services Licence.[3] This will likely remain an area of particular focus for ASIC in light of several high profile data breaches in major companies in the telecommunications and insurance sectors (as discussed further below). This is similarly a focus of the Australian Consumer and Competition Commission (**ACCC**), with the Chair of the ACCC noting on a conservative estimate that Australians were defrauded of AUD1.8 billion in 2021.

– **Product design and distribution** – to increase compliance with regulations and reduce the risk of harm to consumers of financial and credit products caused by poor product design and distribution practices. ASIC fined a bank a combined penalty of AUD113 million for poor product design and distribution practices, which resulted in consumer harm such as the overcharging of interest on credit card debt.

– **Retirement decision making** – to protect consumers as they plan for retirement, focusing on relevant financial products and advice.

See more detail in our blog on sustainable finance, governance and greenwashing.

Developments at Australia's competition regulator

The ACCC's strategic priorities complement ASIC. It also focuses on environmental claims and sustainability as well as consumer and competition issues in the digital economy[4].

Law reforms impacting corporate criminal liability

New National Anti-Corruption Commission

An Act establishing a new National Anti-Corruption Commission was passed on 30 November 2022, with the new Commission expected to be formed in mid-2023. The Commission will be empowered to investigate serious corrupt conduct in the federal public sector.

It will investigate corporations and their officers insofar as they may have adversely affected the honest or impartial exercise of a public official's powers, functions or duties.

There are a number of key concepts which create uncertainty. For example, in order to commence an investigation the Commission must be of the opinion that possible corruption is '*serious or systemic*', concepts which are not defined.

These uncertainties carry real risks for corporates engaging with the Federal Government.

Increased penalties for privacy breaches

Following major data breaches within the telecommunications and insurance sectors, the Government has introduced a Bill to significantly increase penalties for serious or repeated privacy breaches. Maximum penalties for breaches of the *Privacy Act 1988* (Cth) will increase from the current AUD2.22m to whichever is the greater of:

– AUD50m;

– three times the value of any benefit obtained through the misuse of information; or

– 30% of a company's adjusted turnover in the relevant period.

2 https://asic.gov.au/about-asic/corporate-publications/asic-corporate-plan/.

3 ASIC v RI Advice Group Pty Ltd [2022] FCA 496; see also our article discussing this case: https://www.allenovery.com/en-gb/global/blogs/investigations-insight/managing-cyber-security-risks-key-learnings-from-australias-first-test-case.

4 https://www.accc.gov.au/about-us/australian-competition-consumer-commission/our-priorities/compliance-enforcement-policy-and-priorities#:~:text=2022%2D23%20priorities,-Our%20enforcement%20and&text=Consumer%20and%20fair%20trading%20issues,from%20the%20COVID%2D19%20pandemic.

The Bill will also grant the Office of the Australian Information Commissioner (**OAIC**) powers to request information about a data breach, assess a corporate's compliance with the notifiable data breach scheme and disclose information and documents to third parties, including the general public where it is in the public interest to do so.

These reforms sit alongside ASIC's strategic priority on technology risks, discussed above, and its willingness to take enforcement action against companies which fail to have adequate cybersecurity processes and procedures in place.

Financial Accountability Regime

Two new Bills are aimed at implementing recommendations from the 2018 Royal Commission into Misconduct in the Banking, Superannuation and Financial Services industry. The Bills will create a Financial Accountability Regime (the **Regime**) that seeks to improve the operating culture of companies in this sector by imposing obligations on:

- Accountability – requiring entities, their directors and most senior and influential executives, to conduct business with honesty, care, skill and diligence.
- Key personnel – requiring entities to nominate senior executives to be responsible for all areas of their business operations.
- Deferred remuneration – requiring entities in the industries to defer at least 40% of the variable remuneration of directors and senior executives for a minimum of four years and reduce their variable remuneration for non-compliance with their accountability obligations.
- Notification – requiring entities to provide the Regulator with certain information about their business, directors and most senior and influential executives.

The Regime will be jointly regulated by ASIC and APRA (Australia's prudential regulator).

A breach of an obligation by a corporation may result in a maximum penalty of at least AUD11.1m. Individuals who are deliberately involved in a contravention may also be liable under the ancillary contravention penalty provisions, with a maximum penalty of at least AUD1.1m.

New Powers for ASIC

Since October 2021, issuers and distributors of financial products have been required to publish Target Market Determinations (**TMD**) that set out the class of consumers a financial product is likely to be appropriate for.[5] To accompany these new obligations, ASIC's regulatory toolkit has been expanded to include Product Intervention Powers and Stop Orders. These new enforcement tools enable ASIC to temporarily order a company to refrain from engaging in certain conduct in relation to issuing or distributing financial products. ASIC has signalled that it considers that these new powers will be a significant tool in the protection of consumers. We expect to see increased enforcement of TMD obligations and the use of these new powers in 2023.

Increased and new penalties for competition offences

On 1 November 2022, the ACCC welcomed significant amendments to the Competition and Consumer Act 2010, including the Australian Consumer Law, with the recent passage of the *Treasury Laws Amendment (More Competition, Better Prices) Bill 2011.*

Major amendments to the competition enforcement regime are twofold:

- First, **significant increases in maximum penalties** for relevant breaches of the competition and consumer laws; and
- Second, the introduction of penalties and other changes relating to unfair contract terms.

Under the changes, the new maximum penalties for companies that breach relevant provisions of the competition and consumer law are the **greater** of:

AUD50m	This is a five-fold increase from the current AUD10m
Three times the value derived from the relevant breach	This is unchanged from the current position
30% of the company's turnover during the period it engaged in the conduct (if the value derived from the breach cannot be determined)	This is an increase from the current position of 10% of annual turnover in the 12 months prior to the breach

5 https://treasury.gov.au/consultation/c2019-t408904/update-ddo-regime

For individuals, the maximum penalty will increase to AUD2.5m (from AUD500,000 presently).

These penalties apply to a range of offences and civil penalty provisions under the Australian Consumer Law, including: unconscionable conduct, false or misleading representations, harassment and coercion, products that do not comply with safety or information standards, and more.

The penalties also apply to most civil and criminal offences under the competition law, including: cartel offences, the news media bargaining code, international liner cargo shipping provisions, and prohibited conduct in the energy market provisions.

The changes introduce the **first-ever penalties for businesses that include unfair contract terms** in their standard form contracts with consumers and small businesses. Previously, the courts could declare specific terms of a contract unfair and therefore void, but they were not prohibited and courts could not impose any penalties on businesses that included them in the standard form contracts.

The penalty provisions only apply to new contracts, or existing contracts (once **renewed or varied**), made at the end of the 12-month grace period after Royal Assent.

Further, the changes will also expand the coverage of the unfair contract terms regime to more small business contracts, will apply irrespective of the value of the contract, and clarify other aspects of the laws including more clearly defining 'standard form contracts'.

Anti-Money Laundering and Counter-Terrorism Financing Amendment (Making Gambling Businesses Accountable) Bill 2022

Recent anti-money laundering reforms have been proposed in the wake of several reviews into Australia's two largest casino operators. The proposed amendments impose a positive obligation on entities which provide gambling services to report to AUSTRAC (Australia's financial intelligence agency) if they have reason to suspect a person is betting with 'stolen property'. It is proposed that this be a civil penalty provision.

Internal investigations – key considerations

Regulators have continued to challenge legal professional privilege claims made by companies over documents which would otherwise have been disclosable.

In a recent case brought by the Australian Taxation Office (**ATO**), the Court found that a large consultancy firm incorrectly claimed legal privilege over a large number of documents. The ATO argued that the company had attempted to involve lawyers purely for the purpose of covering work in a 'cloak of privilege'. Ultimately, the judge found that the assessment of privilege must be conducted for each document individually, as simply routing documents through the inbox of a lawyer would not mean that the documents would attract privilege.[6]

Similar criticisms were also made by Counsel assisting in a high profile public Commission of Inquiry into one of Australia's largest casino operators.

Companies should continue to bear in mind that communications by a lawyer will not necessarily attract legal privilege, and that regulators continue to aggressively interrogate claims of privilege by individuals and companies. As always, a document by document analysis of the 'dominant purpose test' is required.

6 https://www.afr.com/companies/professional-services/ato-puts-law-firms-on-notice-after-landmark-pwc-privilege-case-20220404-p5aali

Sectors targeted by law reforms or enforcement action

The gaming, telecommunications and insurance industries have been the subject of regulatory scrutiny and have been targeted for law reform.

Two significant data breaches by leading companies in the telecommunications and insurance sectors resulted in the personal data of millions of Australians being compromised. Some of this is very sensitive personal data, for example, data relating to government issued identification documents and detailed health data. Some data has been released on to the internet and has been used to extort some of the people affected.

We expect these data breaches will result in all sectors being subject to increased regulatory scrutiny of the justification for, and measures taken to protect, personal data held by companies.

Technology risks have already been identified as a strategic priority for ASIC and reform has already been made to the *Privacy Act 1988* to strengthen the penalties for contravention of the Act. In addition, the Government has increased its budget allocation for OAIC to support its response to the recent data breaches and OAIC has indicated that it has 'shifted to a stronger enforcement posture in line with increased privacy risks and the community's growing concerns over the protection of their data'.[8]

The gaming industry has been under particular scrutiny. Significant AML failures have been identified at both of Australia's major casinos. Law reform has already been proposed and it is likely that more will follow although the impact to industries outside the gaming industry remains unclear.

Cross-border coordinated investigation or enforcement activity

Information sharing and operational coordination has been a priority for Australia's key regulators, including the ACCC and ASIC. This has extended to cooperation with regulators in other jurisdictions. For example, the Australian Federal Police (**AFP**) in a recent investigation into alleged bribes paid by two Australians to foreign officials to obtain construction contracts in Sri Lanka involved coordination with the FBI, Royal Canadian Mounted Police, and authorities in India, Sri Lanka and Bangladesh.[9]

There has been increasing cooperation between the AFP and the Serious Fraud Office (**SFO**) in the United Kingdom, where requests were made by the AFP to obtain evidence gathered in the context of a bribery investigation carried out by the SFO.

7 https://www.oaic.gov.au/updates/news-and-media/oaic-welcomes-additional-budget-funding-2022

8 https://www.afp.gov.au/news-media/media-releases/two-sydney-men-charged-conspiracy-bribe-foreign-officials#:~:text=Two%20Sydney%20men%20are%20due,in%20September%20of%20this%20year

Predictions for 2023

Sanctions enforcement

Similar to other jurisdictions, this year saw significant changes to Australia's Autonomous Sanctions regime. Russia's invasion of Ukraine and the new *Magnitsky-style* sanctions reforms introduced at the end of last year may result in difficulties for corporates navigating this changing landscape.[10] Falling in line with other countries, Australia has established a dedicated intelligence unit that will sit within AUSTRAC to monitor compliance with sanctions against Russia. Companies should conduct regular reviews of their compliance risk policies and procedures to ensure their sanctions regime remains up to date as these developments make it a likely target for increased regulatory focus.

Greenwashing

In line with regulatory developments globally, greenwashing will be a priority area of regulatory focus for ASIC. Companies offering sustainability-related products will need to pay particular attention not to fall foul of the prohibition against misleading and deceptive conduct. In June 2022 ASIC advised that vague terminology and inadequate explanations should be avoided when communicating information about sustainability-related products to the market.[11]

On 27 October 2022 ASIC took its first action against a company for greenwashing.[12] ASIC's prompt response signals to the market that it is closely monitoring companies and will take enforcement action for any breaches. In house legal teams should take a cautious approach with respect to sustainability-related products and ensure that any communication to shareholders, members and the market is accurate and has a reasonable basis.

Separately, we note that, with recent leadership changes at ASIC, the Australian Competition and Consumer Commission (**ACCC**) and the Australian Prudential Regulatory Authority (**APRA**), there may be changes on the horizon for Australia's enforcement landscape.

9 https://www.dfat.gov.au/news/news/autonomous-sanctions-amendment-magnitsky-style-and-other-thematic-sanctions-act-2021

10 https://asic.gov.au/regulatory-resources/financial-services/how-to-avoid-greenwashing-when-offering-or-promoting-sustainability-related-products

11 https://asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-294mr-asic-acts-against-greenwashing-by-energy-company

Key team members

Jason Gray
Partner – Sydney
Tel +612 9373 7674
jason.gray@allenovery.com

Angus Ryan
Senior Associate – Sydney
Tel +612 9373 7751
angus.ryan@allenovery.com

Pamela Vassil
Lawyer – Sydney
Tel +612 9373 7569
pamela.vassil@allenovery.com

Karen Chow
Graduate-at-Law – Sydney
Tel +614 8801 7339
karen.chow@allenovery.com

"Jason is clearly a subject matter expert when it comes to compliance matters, giving legal advice that is not only compelling but also very much valued."

Chambers Asia Pacific, 2022 – Australia, White Collar Crime & Corporate Investigations

"Jason Gray is extremely knowledgeable within the practice area… Very good at adapting to the client brief and delivering an appropriate solution, nothing over-engineered."

Asia Pacific Legal 500, 2021 – Australia, White Collar Crime

"Jason is very hands-on, very commercially aligned with our objectives, and very easy to work with."

Asia Pacific Legal 500, 2022 – Australia, White Collar Crime

Belgium

Regulatory and criminal enforcement in Belgium remains robust, with a significant uptick in the investigation and prosecution of corruption, environmental pollution, social fraud and human trafficking. Authorities are in particular focusing on the chemical, construction and transportation sectors.

Looking ahead, we expect this trend to continue and intensify in light of: (i) increased regulation (such as the development of a Business and Human Rights framework and the expected introduction of ecocide as a self standing criminal offence under the new Belgian Criminal Code); (ii) compliance, in the broadest sense of the word, becoming a focal point for businesses in any sector; and (iii) increased whistleblowing disclosures, driven by the very recent transposition of the EU Whistleblowing Directive into Belgian national law.

Financial crime remains high on the cross-border enforcement agenda, and will only gain in importance due to the rapidly increasing caseload of the European Public Prosecutors Office (**EPPO**), increased enforcement activities by financial market regulators and antitrust authorities and recent calls for EU Member States to enforce the myriad of sanctions imposed in response to Russia's invasion of Ukraine.

Investigations trends/developments

International sanctions (including EU efforts to increase criminal enforcement)

The EU's response to the war in Ukraine (as with the responses of the UK, the U.S. and other countries) has demonstrated that sanctions will remain at the forefront of international policymaking, with an important impact on Belgian businesses with an international footprint. The array of sanctions adopted in 2022 has been unprecedented, and we have seen many businesses struggling with the compliance burden of navigating this complex landscape. Looking ahead, and with these sanctions here to stay, we expect an uptick in sanctions enforcement, including criminal prosecutions.

EU criminal law – rising amount of cases by EPPO: focus on different types of (cross-border) fraud

The EPPO started its activities in June 2021, and has opened more than 1000 investigations across the EU since then. In Belgium alone, it has initiated over 25 investigations into criminal conduct that have allegedly caused more than EUR320m in damage. As a result of the activities of the EPPO, we expect an increase in cross-border fraud investigations in Belgium, notably in customs matters. In cases that are prosecuted by the EPPO, criminal court litigation will be the preferred option, and out-of-court settlements and dismissals will be the exception.

Social criminal law topics – including issues with (sub)contractors

There has been an increased use of both subcontracting and posted foreign workers in the Belgian labour market. Problems relating to social fraud and social dumping have caused the Belgian authorities to increase their scrutiny of this phenomenon. Belgian social law chain liability schemes have further incentivised large-scale investigations by Belgian prosecutors, as principals may be held civilly liable for the underpayment of wages by their (sub)contractors and for the payment of social security contributions on these unpaid wages. Companies may also be directly targeted for criminal prosecution if their knowledge of illegal employment by a (sub)contractor on Belgian territory can be demonstrated. Recent high-profile cases in several sectors have been widely discussed in the media, resulting in significant reputational damage, following initial undercover media reports alleging various social malpractices by subcontractors. This has led to inspectorate raids triggering investigations, at times into directors and C-suite executives, concerning allegations of social criminal law offences such as leading a criminal organisation or aiding or abetting human trafficking.

Whistleblower directive – transposition in Belgian law

The new EU Directive on the protection of persons who report breaches of Union law (the **EU Whistleblowing Directive**) was adopted in 2019, with a requirement that EU Member States transpose the EU Whistleblowing Directive into national law by 17 December 2021. Like many other EU Member States, Belgium has missed this deadline, but the transposition of the EU Whistleblowing Directive into Belgian national law was finally realised with the Belgian whistleblowing law that will enter into force on 15 February 2023.

The Belgian whistleblowing law has a broader material scope than the EU Whistleblowing Directive. It makes anonymous reporting possible via an external channel and via an internal reporting channel at companies with more than 250 employees. The law provides for an extensive out-of-court protection procedure for the settlement of conflicts between the victim of retaliation, and the entities or persons who retaliate.

As whistleblowing was not regulated in Belgium before (with some exceptions for the financial and public sectors), we expect an increase in the number of reports and, as result, in the number of investigations following the entry into force of the Belgian whistleblowing law.

Increase of compliance risks/burden/awareness on multiple fronts – companies are proactively tackling this

Expectations that private actors will have to conduct due diligence on their customers and supply chains, implement appropriate screening measures and issue public reports on internal processes and their implementation, continue to increase. Businesses need to screen their partners for different categories of risks, including in relation to international sanctions, money laundering, bribery and corruption, and risks of adverse sustainability and human rights impacts in their supply chains. In recent years, we have seen that businesses across all sectors are proactively handling these new compliance challenges by strengthening their compliance frameworks, which raises market standards and puts businesses who do not do so at an increased liability risk.

Law reforms impacting corporate criminal liability

Ecocide

A new code of criminal law is expected to introduce radical changes to the Belgian criminal law system. Under the current proposal, penalties for already existing offences will be revised and streamlined, and new criminal offences, including a self-standing offence of 'ecocide', will be introduced. These legislative developments are in line with an ever increasing focus on investigating and prosecuting environmental pollution.

Transposition of Whistleblower directive

The Belgian whistleblowing law provides for criminal sanctions for non-observance of the rules on the internal reporting channel, and registration of the reports.
This will also provide criminal sanctions for legal entities, its employees, and every natural person or legal person who:

- hinders or attempts to hinder reporting
- retaliates against protected persons
- brings vexatious proceedings against protected persons
- breaches the duty of maintaining the confidentiality of the identity of reporting persons.

In line with the EU Whistleblowing Directive, it also imposes sanctions when reporting persons have knowingly reported or publicly disclosed false information.

Corporate sustainability reporting and due diligence directives

The year 2023 will be marked by the development of a wide array of new sustainability obligations for companies operating in the EU. While the scope of the future Corporate Sustainability Due Diligence Directive, introducing mandatory human rights and environmental due diligence obligations, is still under discussion, the Corporate Sustainability Reporting Directive was adopted on 28 November 2022, thereby extending companies' previous obligations under the Non-Financial Reporting Directive. While it remains to be seen how this new directive will be implemented in Belgian law, there is little doubt that the Belgian legislator will maintain the criminal liability to which non-compliance with the obligations resulting from the Non-Financial Reporting Directive gave rise.

On corporate due diligence, Belgian lawmakers have maintained the proposed criminal liability regime in the amendment to the Belgian draft law on corporate vigilance and responsibility introduced in August 2022. Further parliamentary debate on the draft law is likely not to take place before the Corporate Sustainability Due Diligence Directive is adopted at EU level.

Sectors targeted by law reforms or enforcement action

The fight against social fraud and illegal employment remains an enforcement priority in Belgium. The transport and construction sectors (among other sectors) are being specifically targeted by the Social Intelligence and Investigation Service (the **SIOD**) as high risk sectors for social fraud and social dumping.

As a result, and as in previous years, so-called flash audits have been carried out in 2022 (and possibly again in 2023) in these sectors. Such flash audits typically focus on the payment of (minimum) wages and social security contributions, documentary requirements and working time limitations. We see these audits resulting in criminal prosecutions not only for a breach of social laws, but also for common law criminal offences such as forgery, criminal organisation and human trafficking.

Businesses that are subject to these kinds of investigations face serious reputational risks.

Cross-border coordinated investigation or enforcement activity

EU criminal law statistics: increased efficiency of cross-border investigations

After a year of existence, 928 cases have been opened, of which around 30 have been referred to national courts, mainly concerning VAT fraud.

A majority of these investigations target alleged cross-border criminal conduct. As these first investigations progress and new investigations are opened, we expect to see an uptick in criminal enforcement actions and litigation in relation to cross-border fraud, including in customs matters.

Increase in cross-border workplace investigations

There has been an increase in workplace investigations with a cross-border dimension in 2022. As a result of the international activities of companies, employees in several jurisdictions may be involved. Therefore, the laws of multiple jurisdictions govern the investigative process. Different local counsel must be consulted as to how the investigation must be conducted to comply with local laws. The need for cross-border engagement is further strengthened when the investigation also entails carrying out an exercise to assess the culpability of (a group of) employees who are subject to different local rules in terms of possible disciplinary measures and procedures.

Predictions for 2023

Social criminal law topics

In-house legal and investigation teams must demonstrate an increased awareness of social fraud and social dumping, which have significant potential to bite through the chain liability systems prevalent in Belgian social law. Once these systems are triggered, for example, when a construction project is set up, they may have far-reaching consequences for companies making use of (sub)contractors, even if the infractions are limited to a lower-tier supplier, resulting in the company being exposed to civil and even criminal liability. Combined with the anticipated new rules on whistleblowing, which we expect to lead to an uptick in reports, this means that it is vital to have a clear and in-depth system of vetting with a unified process. Moreover, the chain of subcontractors needs to be mapped and monitored in order to prevent undeclared work, and ensure the payment of wages and social and fiscal debts.

Greenwashing claims and enforcement action

Although no such claims have been directed at corporates in Belgium, we do expect Belgium to follow neighbouring countries, with greenwashing claims and/or enforcement actions against companies and their directors by regulators, prosecutors and shareholders.

EU criminal law (including sanctions)

For a few years now, there has been a clear policy at EU level to boost the criminal enforcement of legal violations that violate EU interests. Besides the investigations initiated by the EPPO, the European Commission is taking steps to harmonise and strengthen the criminal enforcement of EU sanctions laws, and is openly calling on Member States to step up enforcement.

Key team members

Joost Everaert
Partner – Brussels
Tel +32 2 780 26 06
joost.everaert@allenovery.com

Inge Vanderreken
Partner – Brussels
Tel +32 2 780 22 30
inge.vanderreken@allenovery.com

Camille Leroy
Senior Associate – Brussels
Tel +32 2 780 2493
camille.leroy@allenovery.com

Thomas Declerck
Senior Associate – Brussels
Tel +32 2 780 2483
thomas.declerck@allenovery.com

Basil Saen
Associate – Brussels
Tel +32 2 780 2523
basil.saen@allenovery.com

Mathias Vandenhoudt
Associate – Brussels
Tel +32 2 780 22 59
mathias.vandenhoudt@allenovery.com

Ellen Permentier
Senior Knowledge Lawyer – Brussels
Tel +32 2 780 24 65
ellen.permentier@allenovery.com

"The practice further boasts strength in white-collar crime matters, advising clients on criminal investigations and litigation relating to allegations of money laundering, bribery and fraud."

Chambers Dispute Resolution, 2022

"The practice is capable of handling very large and complex cases. They cooperate very well and have the most advanced technology. Client communication is a real plus."

Legal 500 Fraud and White Collar Crime, 2022

"Allen & Overy are widely recognised for their considerable expertise in handling a range of criminal cases, including sporting fraud and cybercrime."

Legal 500 Fraud and White-Collar Crime, 2022

Mainland China

China's data laws add substantial complexity to the cross-border transfer of documents and evidence for investigations, particularly in the context of requests from foreign government authorities, and for internal investigations. This will impact how a company can respond to direct requests from non-Chinese authorities in any investigation concerning China-based conduct. Data enforcement activity is also increasing rapidly, and has confirmed that foreign-registered entities are captured squarely by the PRC data regime, if processing activities under their direction are carried out in China.

A dip in ABAC enforcement activity against companies in 2022, due to competing governmental priorities (notably Covid), is expected to be temporary, with the government regularly restating its commitment to combat both active and passive bribery.

China's approach to the regulation of non-fungible tokens (**NFTs**) is evolving, and it is expected that regulation will include ensuring that NFTs are not commoditised, in line with China's approach to cryptocurrencies.

Investigations trends/developments

A low ebb in anti-bribery and anti-corruption (ABAC) enforcement actions

Following a trend that started in 2021, the number of published ABAC-related enforcement cases continued to decline in 2022. *China Judgments Online* reported 34 first-instance bribery convictions as of late October 2022, as compared to 158 in 2021. The real estate and construction industries continued to account for around one third of these cases in 2022. Similarly, according to a Wolters Kluwer database, the number of published administrative penalty decisions for commercial bribery dropped from 100, in 2021, to 40 in the first ten months of 2022.

While China continues to crack down on passive bribery and graft by removing and sentencing high-level public officials, including (as of August 2022) four ministerial-level officials, 21 vice-ministerial-level officials, and several senior executives of centrally state-owned enterprises, there have been no high-profile enforcement actions against companies committing active bribery. This is particularly noteworthy as the government declared in the last year that it would be more active in punishing active bribery, and in pursuing further "concurrent investigations" of active and passive bribery.

This decline in commercial enforcement action may be due to a shift in the government's priorities towards more urgent threats, including international political pressures, and COVID and its associated preventive measures.

During the pandemic, there was a significant expansion of government power at both the central and local levels. At the same time, the "emergency" nature of this more expansive government reach has complicated the ABAC environment in China, as parties balance their compliance obligations with the need for urgency in dealing with the government's epidemic controls.

We expect this trend of lessened enforcement action to be temporary, with the government regularly reaffirming its commitment to the "anti-corruption" campaign. The critical and unanswered question is when the government will turn its attention back to ABAC as a policy priority. It is interesting to note that, on 22 November, the State Administration for Market Regulation (**SAMR**) released a new draft amended version of the *Anti-Unfair Competition Law* (the **AUCL**) for comment. The new draft proposes reinstating a previously-abandoned, controversial approach to punishing active bribery directed not only at the personnel of transaction counterparties, but also at transaction counterparties themselves (if not properly accounted for). It also proposes reinstating punishment for passive bribery, and strengthening the administrative penalty for violations.

A giant leap in data law enforcement

China's regulators have been far more active in enforcement of its new data protection laws. The new data regime saw its most high-profile enforcement action to date in July 2022, when the Cyberspace Administration of China (**CAC**) announced a fine of RMB8.026bn against Didi Global Co., Ltd., for various data-related violations including: (i) unlawful or excessive collection of personal information; (ii) processing of personal information without adequate notification; (iii) frequent requests for permission from data subjects without justification; (iv) inaccurate and unclear description of purposes for processing personal information; and (v) carrying out data processing activities that harm national security and the security of China's critical information infrastructure. This case has also highlighted CAC as another significant regulator in China's regulatory regime that requires special attention.

In addition to the gravity of the penalty, this case has raised several issues worth noting:

– Didi Global Co., Ltd. was found to be the offender even though it is the offshore parent company of the onshore operational entities of the Didi Group. It is therefore confirmed that foreign-registered entities are captured squarely by the PRC data regime, if processing activities under their direction are carried out in China.

– CAC adopted strict criteria in determining whether c ertain of the processing activities were "necessary" and "minimal." We note that the collection of certain personal information, eg access to phone numbers of the passengers using the service) was not without business justification, but was nonetheless determined to be "excessive".

– It remains unclear how the fine was calculated, and, in particular, if the fine included confiscation of illegal income. Additionally, while the amount of the fine was high, the regulators actually did not resort to the more disruptive penalties in their toolbox, such as suspension of business, revocation of the business licence, negative entry in the social credit records, disqualifying the responsible individuals from certain senior roles in the company, and pursuit of criminal liability, presumably due to the importance of Didi's services in the Chinese market. That is not the case in other enforcement actions, however, with the CAC issuing a public announcement, on 3 November 2022, that it had recently terminated the operation of 55 mobile applications and ordered timely rectification by another 80 mobile applications, for various data violations.

For more information about the Didi case, please refer to our previous article published at https://www.linkedin.com/posts/aosphere_cac-imposes-rmb-8026-billion-fine-on-company-activity-6956200535427317761-ezu0.

De-commoditisation of NFTs

The market for non-fungible tokens (**NFTs**) has expanded significantly in China since 2021, as it has in many other places around the world. NFT market players in China are not limited to private sector enterprises, with many players having a government background. The former includes tech giants such as Tencent, Alibaba, and Baidu, which have all launched NFT marketplaces. The latter includes Xinhua News Agency and China Central Television, which have developed and issued their own NFT products, and government-sponsored cultural artwork exchanges seeking to set up online trading platforms for NFT-based digital artworks.

It is unsurprising that China has taken a dim view of attempts to commoditise or securitise cryptocurrencies, through initial offerings, trading, and speculation. NFTs, which often rely on blockchain technology and are often associated with cryptocurrencies, are likely to be regulated under the same principles.

Other than the general regulation on "blockchain-based information service providers," NFTs have not been subject to any special regulations so far. However, industrial associations including the National Internet Finance Association of China, the China Banking Association, and the Securities Association of China jointly issued the Proposals on *Preventing NFT-related Financial Risks* in April 2022, which set forth basic principles for NFT-related businesses, with a focus on rebuffing the attempts to commoditise or securitise NFTs. While these industrial associations are not government regulators, and the Proposals have no legal effect, the Proposals may be viewed as "testing the waters", and may shed light on future legislative direction.

Many key onshore market players have adopted the following measures to minimise the financial attributes of NFTs, in order not to be considered as engaging in illegal securities issuance, fundraising or exchange of business, or violating the cryptocurrency and Initial Coin Offering ban in general:

– tokenising artworks on the consortium blockchain rather than the public blockchain

– referring to NFT products as "virtual collectibles" instead of "tokens" to avoid the apparent association with cryptocurrencies

– prohibiting the use of cryptocurrencies for transactions of NFT products

– suspending secondary trading of NFT products for the time being

– prohibiting any fractionisation of NFT products.

Some of the measures (such as the ban on secondary trading) may be relaxed or lifted as the regulatory framework on NFTs evolves. However, many others are expected to stay as standard industry practices.

Foreign market players are advised to adopt similar measures to the extent possible when providing NFT-related services to Chinese residents, or otherwise engaging in NFT businesses in China, to avoid the attention of PRC regulators.

The Chinese government is also wary of the money-laundering risk arising from NFTs. In the Chinese onshore NFT market, this risk is controlled indirectly from the efforts to decommoditise NFTs, especially by limiting payments to be made through banks or licensed third party payment companies that are AML-obligated persons. The risk is further reduced by the market practice of making NFTs analogous to "collectibles" as opposed to financial assets. However, foreign market players that intend to provide NFT-related services to Chinese residents on a cross-border basis should also be aware of the potential extraterritorial effect of the PRC anti money laundering laws, particularly the criminal laws. For the sake of prudence, foreign market players that intend to provide NFT-related services to Chinese residents are advised to follow the same approach adopted in relation to the Chinese domestic market when doing so.

Important 2022 law reforms impacting corporate criminal liability

As in 2021, 2022 witnessed continuing, significant developments in laws governing the cross-border transfer of data. In general, the PRC data legislation requires, among other things, that data processors shall: (i) pass mandatory government security assessments; (ii) obtain security certifications issued by a government accredited agency; or (iii) execute standard agreements (using the government-issued template) with foreign recipients, before transferring personal information and/or important data abroad. Failure to comply with these rules when transferring personal information and certain other data abroad may lead to administrative liability and, in extreme cases, criminal liability.

CAC released, on 7 July 2022, the long-awaited *Measures on Security Assessment for the Cross-border Transfer of Data* (the **Security Assessment Measures**) in order to flesh out the security assessment process briefly referred to in the data laws. The Security Assessment Measures articulate the conditions under which a security assessment is required, the procedures for security assessment, and the factors that the authorities will consider when conducting a security assessment.

Around the same time, the Secretariat of the National Information Security Standardisation Technical Committee issued the *Security Certification Specification for Cross-border Processing of Personal Information* (TC260-PG-20222A) (the **Specification**), which sets forth principles, rules, and basic requirements for the security certification process. The Specification was updated on 8 November, and the *Rules for the Implementation of Personal Information Protection Certification* jointly released by CAC and SAMR on 4 November specifically require compliance with the Specification for the security certification process.

CAC also released for public comment the draft *Provisions on Standard Contracts for Cross-border Transfers of Personal Information* (the **Standard Contracts Provisions**), which forecast the conditions where cross-border transfer of personal information may be based on standard conditions, and what the government issued template agreement will look like.

With the Security Assessment Measures and the Security Certification Specification now in place, and the Standard Contract Provisions in the pipeline, the main regulatory framework on the cross-border transfer of personal information and important data is in place. After the grace periods, data processors will need to follow the applicable rules and procedures before transferring personal information or important data abroad, and they can no longer avoid compliance while "waiting" for implementation rules.

That said, these cross-border data transfer rules do introduce new questions that will require clarification in the future. For instance:

- it is unclear what the relationship between these general cross-border transfer rules and the pre-existing data transfer review and approval processes developed by industrial regulators is
- the requisite level of detail of the submission materials for security assessment and security certification remains an area of know-how to be developed by practitioners, based on their first-hand interactions with the regulators
- the legal community is still eager to understand the extent to which data protection agreements between data processors and their foreign recipients that are multinationals will be allowed to deviate from the government template, as there are many issues that will likely arise with execution of the template as it is, particularly with multi-jurisdictional commercial and regulatory considerations in mind.

Internal investigations – key developments

The development of the cross-border transfer rules will complicate internal investigations carried out by multinationals on a cross-border basis, eg the transfer of findings, evidence, and data from local subsidiaries to global headquarters. China has not provided any exception for cross-border transfer of human resources data or data related to internal investigations, and there is no indication that there will be any such exception, although the government may adopt more streamlined procedures for the transfer of the data based on security assessments and the other requisite processes. The other possibility is a state-to-state agreement between Chinese and foreign regulators for the transfer of such data, although there is no indication that any such agreements are anticipated in the near future.

We and our clients continue to follow these developments closely, as they will directly impact how to conduct both internal and regulator-facing investigations, and how we can cooperate with foreign regulators examining China-based conduct.

Sectors targeted by law reforms or enforcement action

The developments in the data law regime will disproportionally affect industries that are data-intensive, such as finance, e-commerce, social media, smart electronics/terminals, and travel and hotels.

That being said, the data regime is far-reaching, and has already had a demonstrable impact on nearly all sectors doing business in China.

Key team members

Eugene Chen
Registered Foreign Lawyer
– Hong Kong
Tel +852 2974 7248
eugene.chen@allenovery.com

Jane Jiang
Partner – Shanghai
Tel +86 21 2036 7018
jane.jiang@allenovery.com

Yihan Zang
Lang Yue – Senior Associate
– Shanghai
Tel +86 21 2067 6848
yihan.zang@allenoveryly.com

Eugene Chen of Allen & Overy's Hong Kong office is regularly enlisted by pharmaceutical and life sciences companies for assistance with U.S. investigations and anti-corruption and anti-bribery compliance. One client refers to him as a "great white-collar lawyer," while another source considers him a "good guy and a solid lawyer".

Chambers Greater China Region 2022, China – Corporate Investigations/Anti-Corruption

Jane Jiang advises clients on contentious regulatory matters. A client notes that "Jane in particular provides very useful, well-considered, practical and experienced insight into complicated issues". Another client notes that while she is "knowledgeable across the board," she "tells me when she can't do something, which is something that really makes me trust counsel; I always feel like I'm getting sound, sensible, implementable advice".

Chambers Greater China Region, 2022 – China, Financial Services

Eugene Chen has "depth of expertise in U.S. and China anti-bribery work, broad experience across sectors and very personable engagement with clients."

Chambers Asia-Pacific, 2021 – China, Corporate Investigations/Anti Corruption

"Jane Jiang is amazing. Her technical wizardry combined with her client skills makes her a go-to advisor on PRC law matters."

Legal 500, 2022 – China, Regulatory/compliance: Foreign firms

France

France remains a key player in white collar enforcement in Europe. In line with previous years, the fight against money laundering, tax evasion and corrupt practices remains an enforcement priority, in particular for the National Financial Prosecutor's Office (**PNF**). Corporate responsibility for human rights violations has also been a major enforcement and investigations theme this year with the *Cour de Cassation* (the French Supreme Court) and the Paris Court of Appeal upholding unprecedented indictments against corporates for aiding and abetting war crimes and crimes against humanity. There has also been an ever growing number of French style Deferred Prosecution Agreements (*Convention Judiciaire d'Intérêt Public* (CJIP)).

Investigations trends/developments

A strong focus on tax fraud and laundering the proceeds

Tax evasion by corporates was both a focus during the 2022 presidential and legislative elections and for enforcement activity. The PNF, in close cooperation with the French Tax Authorities, directed most of its attention at fighting tax fraud and illicit laundering of proceeds this year.

The harsh penalties handed down in recent cases, mostly settled by way of CJIP, are testimony to the rigorous approach taken by French enforcement authorities in this area:

– A large Swiss bank agreed to pay a total of EUR238m as a public interest fine and for damages to put an end to an investigation opened in 2016 for aggravated laundering of the proceeds of tax fraud and illicit solicitation of customers in France. The ambit of this CJIP, reached in October 2022, covers tax fraud and illicit solicitation, between 2005 and 2012, of thousands of French customers to open undeclared accounts in its books, representing up to EUR2bn in assets.

– A large U.S. fast food corporation and the PNF agreed on a EUR1.245bn CJIP in June 2022 to settle an investigation targeting the company's transfer pricing policies.

Also in 2022, in a landmark case, the Paris Criminal Court convicted 14 individuals, made up of hedge fund directors and managers, as well as a tax attorney, working with or at a major U.S. bank, who allegedly took part in setting up a complex optimisation tax scheme using a profit-sharing entity that would have enabled them to avoid paying millions of euros in taxes on investment gains in 2007 and 2008.

The rise of prosecution against corporates for aiding and abetting war crimes and crimes against humanity

Two landmark judgments handed down by the Paris Court of Appeal, following rulings by the French Supreme Court, confirmed the trend towards greater scrutiny and accountability of corporates for human rights violations. The Paris Court of Appeal confirmed the indictments of two corporates for having 'aided and abetted' war crimes, and crimes against humanity. In particular, within two separate proceedings, the Court found that:

– a technology company that produces tools for intercepting communications and analysing data could be indicted for aiding and abetting acts of torture for having, in substance, sold surveillance devices to the Libyan intelligence apparatuses during the time of Muammar Gaddafi's reign.

– a large cement company could be indicted for aiding and abetting crimes against humanity for allegedly having, in substance, paid bribes to local terrorist groups, including to ISIS, through its Syrian subsidiary, with a view to allowing its local factory to continue its activities in Syria up until 2015.

This trend can also be tied to the increase in compliance duties imposed on large businesses regarding human and environmental rights, such as, but not limited to, the "duty of vigilance" rule and the increased accountability for corporates in relation to their ESG commitments. For example, recently a large French bank was threatened with climate litigation for allegedly having insufficiently identified the human and environmental impacts of its fossil fuel financing operations, as would have been required by the corporate "duty of vigilance" rule. Likewise, we are seeing more complaints targeting corporates on the grounds of potentially misleading commercial practices, and for allegedly failing to fully comply with their own ethical commitments.

French-style DPAs

Since the CJIP was introduced by the "Sapin II" law in late 2016, the number of settlements for corporates has steadily risen and become a key part of the French enforcement environment.

The widening of the scope of the CJIP to tax fraud in 2018 and environmental offences in 2020, is testimony to its success.

In 2022 alone, 14 CJIP were signed and validated by the competent courts, and over EUR1.3bn was handed down as public interest fines and damages. More are currently being negotiated, such as a recent bribery settlement between an aircraft manufacturer and French authorities over past dealings in Libya and Kazakhstan.

Significant law reforms impacting corporate criminal liability

Evolving case law on excessive length of criminal proceedings

White collar crime investigations in France have historically been very lengthy. After a recent push from lower courts to declare null and void proceedings that were considered to have lasted for an "unreasonable time", the French Supreme Court put an end to this trend on 9 November 2022, in the *Chaufferie de la Défense* case relating to corruption allegations, ruling that:

– the excessive length of criminal proceedings does not in and of itself justify its annulment; but
– it can nonetheless have consequences on the evidentiary value of the elements at hand as well as an impact on sentencing.

Unreasonable delays in cases have become increasingly common in France, particularly in complex financial cases. Such delays raise important questions as to the right to a fair trial.

Potentially stricter framework for criminal investigations

In an attempt to better regulate and limit the duration of criminal investigations, a December 2021 law reform purports to regulate the duration of preliminary investigations (led by the police under the supervision of the public prosecutor) to a maximum of two years from the first investigative act.

This period may be extended by an additional year with the written and documented authorisation of the public prosecutor, and is suspended for the duration of international cooperation requests.

It remains to be seen how these new limitations will impact the way complex white collar crime investigations are run.

Reinforcement of legal privilege

Key principles governing attorneys' legal privilege in France were enshrined in legislation during a large scale reform of the French judicial system in December 2021, which was reviewed and for the most part approved by the French Constitutional Court (*Conseil constitutionnel*). The law now explicitly recognises the existence of attorneys' legal advice privilege, aligned with legal privilege relating to the rights of defence. The law also memorialises a principle from French case law: that attorneys and their clients cannot rely on French privilege where communications between them may have helped perpetrate or facilitate corruption, tax fraud or terrorist financing.

Impossibility of prosecuting both administrative and criminal offences concomitantly

The dual system of administrative and criminal sanctions for obstructing the inspections and investigations of the French Financial Markets Authority (*Autorité des marchés financiers*) was declared unconstitutional by the French Constitutional Court on 28 January 2022.

The court reaffirmed the principle that persons cannot be convicted or subjected to both administrative and criminal proceedings based on the same facts qualified in an identical manner, by sanctions of the same nature, for the purposes of protecting the same public interests.

Internal investigations – key developments

New legislation on whistleblowers

New legislation regarding whistleblower protections was adopted in France in 2022 to implement the EU Whistleblowing Directive. The law, effective in March 2022, improves the protection of whistleblowers in companies with more than 50 employees.

However, the French law goes beyond the European requirements. Previously, France only protected whistleblowers if the facts reported were considered *prima facie* as "*serious and manifest*". The new regime has removed this essential condition, which guaranteed a balance between the nature of the facts reported and the response that needed to be made by corporates, despite the obvious cost to companies.

Furthermore, the new law has done away with the requirement that the facts must be reported internally prior to being reported to outside authorities via external channels.

Lack of prospects for new "Sapin III" legislation

Last year, a new "Sapin III" bill was proposed to, among other things, strengthen the rights of individuals during internal investigations. The MP spearheading this bill did not run for re-election in 2022, and a debate on the bill is yet to be scheduled at the French Parliament. We will be closely monitoring this area.

Sectors targeted by law reforms or enforcement action during 2022

The focus remained on tax fraud. Indeed, in the past year, financial institutions were subject to a number of PNF investigations. A number of controversies relating to the allocation of consultancy contracts to consultancy firms by the French Government also led to greater scrutiny in the consultancy sector. As a result, a large U.S. consulting firm is currently under investigation for tax fraud and laundering the proceeds due to their transfer pricing policy.

For French regulatory authorities, the focus this year remains on compliance with AML/CTF regulations by the financial services sector.

The French Anti-Corruption Agency (*Agence française anticorruption*), which is responsible for ensuring compliance with French anti-bribery and anti-corruption (**ABAC**) regulations, gave a number of interviews and published articles in relation to ABAC compliance by public sector companies, which seem to be a recent focus.

Cross-border coordinated investigation or enforcement activity

The European Public Prosecutor's Office (**EPPO**) became operational on 1 June 2021. After a year of existence, 928 cases have been opened, of which around 30 have been referred to national courts, mainly concerning VAT fraud.

To illustrate the efficiency and scale of the investigations led by the EPPO, on 29 November 2022, the EPPO in cooperation with law enforcement agencies of 14 EU Member States, including France, carried out simultaneous investigative measures, including more than 200 searches, in relation to a complex VAT fraud scheme based on the sale of popular electronic goods. It is estimated that the damages investigated amount to EUR2.2bn.

On top of the EPPO's new European operations, there is still a strong willingness among French criminal authorities to work on cross-border coordinated investigation and enforcement activity.

Predictions for 2023

In a criminal public policy circular published on 22 September 2022, the Ministry of Justice stated that it would focus its efforts, among other more general issues, on environmental offences. As such, the energy and mining sector is likely to be subject to increased scrutiny.

Further, in light of the increased cooperation between the French Tax Authorities and the PNF, we expect the focus to remain on tax-related offences, and, as such, for financial institutions in particular to continue to be key targets of enforcement action, with an increasing level of fines and penalties.

Finally, ESG is an up-and-coming topic in the current enforcement environment. The recent litigation prompted by NGOs is likely to be followed by further disputes over the upcoming year.

Key team members

Denis Chemla
Partner – Paris
Tel +33 1 40 06 53 03
denis.chemla@allenovery.com

Hippolyte Marquetty
Partner – Paris
Tel +33 1 40 06 53 98
hippolyte.marquetty@allenovery.com

Dan Benguigui
Partner – Paris
Tel +33 1 40 06 53 17
dan.benguigui@allenovery.com

Paul Fortin
Partner – Paris
Tel +33 1 40 06 53 50
paul.fortin@allenovery.com

"Allen & Overy is a well-regarded team with extensive experience acting before authorities and criminal courts on investigation matters. The law firm also assists with corruption, fraud and regulatory files. The practice frequently handles cases with cross-border components thanks to the firm's international network."

Chambers Europe – Corporate Compliance & Investigations – 2022

Germany

Prosecution authorities, as well as criminal courts, continue to investigate the cum/ex complex, which has led to further indictments and convictions in 2022. A significant number of banks and audit firms have been raided in connection with these investigations. We expect to see more in 2023.

The criminal trial against the former CEO of Wirecard and other former senior Wirecard managers regarding allegations of fraud, balance sheet manipulation and other offences commenced before the Munich Regional Court in December 2022. The criminal trial regarding the Wirecard case will likely continue throughout 2023.

The Supply Chain Due Diligence Act came into force on 1 January 2023, and we anticipate the first regulatory enquiries into compliance with the new law. The German legislature is expected to pass the Whistleblower Protection Act early in 2023, meaning that the new law would come into force towards the end of Q1/2023.

Investigations trends/developments

The German criminal prosecution authorities will continue their enforcement activities against domestic and international financial institutions, as well as their managers and employees in relation to cum/ex trades in 2023. The investigations and court proceedings have gained further traction after the German Federal Court of Justice (*Bundesgerichtshof*) upheld a judgment of the Bonn Regional Court in July 2021, confirming the defendants' conviction of severe tax evasion due to their involvement in cum/ex trading.

Investigations into Wirecard will also proceed in 2023. The criminal trial against the former CEO of Wirecard and other former senior Wirecard managers regarding allegations of fraud, balance sheet manipulation and other offences will likely continue throughout the year. The Munich Regional Court has scheduled 100 days of hearings for the trial, which is expected only to conclude in 2024.

The German Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht*) will continue its financial reporting enforcement examination of the German housing company, Adler Group. In 2022, the German Federal Financial Supervisory Authority issued two press releases, reporting that the consolidated financial statements of Adler Real Estate AG, as at 31 December 2019, contained errors and that the company's consolidated total assets were overstated by EUR3.9bn.

The German Federal Financial Supervisory Authority's powers to conduct financial reporting enforcement examinations were expanded in 2021 by the Financial Market Integrity Strengthening Act (*Gesetz zur Stärkung der Finanzmarktintegrität*), which was passed in response to the Wirecard case. Several media outlets have also reported that the Public Prosecutor's Offices in Berlin and Frankfurt are conducting criminal investigation proceedings into the Adler Group.

Cyber-crime incidents have continued to rise sharply, according to a report of the German Federal Ministry of the Interior (*Bundesministerium des Innern und für Heimat*) published in October 2022. Several German authorities and major German companies have fallen victim to ransomware attacks. Criminal investigation proceedings into a large number of cybersecurity incidents are ongoing. The German Federal Government plans to expand the Federal Office for Information Security's (*Bundesamt für Sicherheit in der Informationstechnik*) operations to respond to the ever-increasing threats.

Significant law reforms impacting corporate criminal liability

Even though the legal initiative to adopt the wholly new Corporate Sanctions Act (*Verbandssanktionengesetz*) was unsuccessful, the current German Federal Government still intends to revise the existing corporate sanctions rules and implement a legal framework for internal investigations. However, the wording in the coalition agreement suggests an amendment of the existing laws concerning corporate sanctions, rather than the adoption of an entirely new act.

Internal investigations – key developments

The German Federal Labour Court (*Bundesarbeitsgericht*) has acknowledged that companies can claim the costs of an internal investigation, conducted by an external law firm, from an employee in certain circumstances. However, the court has set out strict requirements for such a claim such as a concrete suspicion of serious misconduct as the trigger of the internal investigation and proof of an intentional and serious breach of a significant employment-related contractual duty, or even criminal behaviour, by the relevant employee. It is therefore essential for companies to consider these requirements, in particular documentation requirements, prior to any investigation to safeguard their compensation claims. In another decision, the German Federal Labour Court stated that the two-week period of notice for extraordinary termination of employment begins when the employer's managing director is informed about the facts warranting the termination (eg by virtue of being provided with an investigation report). The German Federal Labour Court also stated that, in the relevant matter, the earlier knowledge of the relevant facts by the employer's compliance function did not trigger the notice period.

Sectors targeted by law reforms or enforcement action

With effect from January 2023, companies operating in Germany and employing 3000 people or more will be subject to an entirely new set of rules obliging them to review their supply chains at least once a year and to enact a supply chain-related compliance management system. The newly imposed due diligence obligations under the Supply Chain Due Diligence Act (*Lieferkettensorgfaltspflichtengesetz*) aim to minimise the risk of infringements of human rights and environmental standards. German companies will have to ensure that their suppliers comply with the regulations. Such a trend is already clearly visible in the market, irrespective of the location of those suppliers. Companies may be increasingly exposed to litigation due to possible private enforcement measures by non-governmental organisations and workers' unions and may even be required to terminate relationships with suppliers. The law will also become directly applicable to German companies normally employing 1000 people or more as of 1 January 2024.

The EU Whistleblower Directive is about to be implemented in Germany by the Whistleblower Protection Act (*Hinweisgeberschutzgesetz*), which, among other things, requires companies with 50 or more employees to set up an internal reporting office and is intended to apply to numerous violations of EU and national law.

The Whistleblower Protection Act will enable whistleblowers to claim damages for any potential retaliation measures. We expect the Whistleblower Protection Act to come into force towards the end of Q1/2023. Companies which do not already have this sort of internal reporting mechanism in place will need to amend their compliance system accordingly.

Money laundering is a priority for the German Federal Government, which intends to set up a new federal authority. The planned German Federal Financial Criminal Police Office (*Bundesfinanzkriminalamt*) is aimed at improving the investigation and enforcement of suspected infringements of anti-money laundering laws. Against the backdrop of the significant extension of the criminal offence of money laundering (Section 261 of the German Criminal Code) in March 2021, we expect more enforcement activity in connection with money laundering in the near future. The German Federal Government may take further steps to improve compliance with anti-money laundering laws in view of recommendations received from the Financial Action Task Force in their Mutual Evaluation Report 2022.

Cross-border coordinated enforcement activity

German criminal prosecution authorities are said to have set up joint investigation teams with their counterparts in other European countries in order to trace the cum/ex transactions throughout Europe. These joint investigations are most likely to persist, alongside the ongoing investigations regarding the cum/ex complex.

Due to the severe fish mortality incident in the river "Oder" in 2022, the competent German Federal and State ministries set up a task force with their Polish counterparts to investigate the matter. However, the investigations were ultimately carried out by two separate expert commissions that also came to different conclusion as to the root cause of the incident. Against this background, environmental associations have demanded to implement a better international cooperation in the course of the final adoption of the EU Directive on combating environmental crime, which is expected in the course of 2023.

Financial crime issue predictions for 2023

We expect a rise in the number of criminal investigations into allegations of money laundering. We also anticipate that enforcement actions into notification requirements vis-à-vis the German Transparency Register, which contains information on the beneficial owners of legal entities, will remain at a high level in 2023. Upon creation of a new Federal Financial Criminal Police Office, additional resources will further increase the focus of enforcement activity in respect of anti-money laundering laws.

We also expect the first regulatory enquiries into compliance with the new Supply Chain Due Diligence Act, which will come into force in 2023. The Federal Office of Economics and Export Control (*Bundesamt für Wirtschaft und Ausfuhrkontrolle*), the competent regulatory authority for the new law, will likely issue detailed guidance on the implementation of the legal requirement, which companies required to comply with the law need to take into account.

In view of the wide-reaching expansion of the European Union's financial and economic sanctions against Russia in response to the country's military attack on Ukraine, we also expect to see enforcement activity by German criminal prosecution authorities into non-compliance with the applicable sanctions regulations. While intentional violations of the European Union's sanctions can be prosecuted as criminal offences under German law, negligent violations of the relevant provisions can be sanctioned as administrative offences.

Key team members

Dr Wolf Bussian
Partner – Frankfurt
Tel +49 69 2648 5571
wolf.bussian@allenovery.com

Jan Erik Windthorst
Partner – Frankfurt
Tel +49 69 2648 5583
jan-erik.windthorst@allenovery.com

Dr Tim Müller
Partner – Frankfurt
Tel +49 69 2648 5996
tim.mueller@allenovery.com

Dr David Schmid
Counsel – Frankfurt
Tel +49 69 2648 5774
david.schmid@allenovery.com

Dr Jasmin Hense
Associate – Frankfurt
Tel +49 69 2648 5444
jasmin.hense@allenovery.com

Paul Matthies
Associate – Frankfurt
Tel +49 69 2648 5768
paul.matthies@allenovery.com

Dr Wolf Bussian, Partner

Ranked in "Best Lawyers"

Dispute Resolution, 2022

Jan Erik Windthorst, Partner

Ranked in "Best Lawyers"

Dispute Resolution, 2022

Dr Tim Mueller, Partner

Frequently recommended lawyer for compliance investigations

JUVE Handbuch, 2022/2023 and JUVE Handbuch, 2021/2022

Dr David Schmid, Counsel

"Rising Star White Collar Crime"

Legal Media Expert Group, 2022

Hong Kong SAR, China

The new Head of Enforcement for the Securities and Futures Commission (**SFC**) may in due course herald a change in regulatory direction and enforcement policy in Hong Kong. Whether or not that occurs, the SFC continues to drive change to better regulate the financial markets. A new consultation proposes changes that would permit the SFC to apply for remedial and other court orders on the basis of disciplinary action rather than breach of certain laws, while the SFC continues to advocate for, and seek to expand its regulatory oversight of, the cryptocurrency sector. Meanwhile, proposed legislative reforms address weaknesses in existing cybersecurity laws and strengthen sanctions.

Important trends or developments

Regulatory and other authorities in Hong Kong remained active in their investigation of misconduct and possible white collar crime in 2021/2022, with a particular focus on targeting "high-impact" cases.

In the quarter ended 30 September 2022, the SFC conducted 433 investigations into white collar crime, including corporate disclosure, corporate mis-governance, insider dealing, intermediary misconduct, market manipulation and unlicensed activities. Intermediary misconduct made up 154 out of the 433 investigations.

There has also been an increase in joint operations between the SFC and other regulatory and enforcement authorities in and outside Hong Kong. For example, as announced on:

- 10 November 2022, the SFC and the Independent Commission Against Corruption (**ICAC**) conducted a joint operation against a sophisticated ramp-and-dump syndicate
- 30 September 2022, 13 people were charged following a joint operation between the SFC and the Hong Kong Police Force (**HKPF**) against a ramp-and-dump syndicate
- 5 July 2022, the SFC and HKPF conducted a joint operation on suspected corporate fraud.

The SFC's disciplinary actions have focused on combating: (i) intermediary misconduct, including IPO sponsor failures, AML-related breaches and deficient selling practices (such as internal control failures); and (ii) corporate fraud, including misapplication of funds.

Meanwhile, the cost of disciplinary fines has continued its upward trajectory since 2015. In the period from April 2021 to March 2022, the SFC disciplined 36 corporations/individuals, imposing aggregated fines of HKD4101.1m.

Outside of enforcement action, the SFC continues to drive investor protection. To this end, the SFC has released a consultation proposing enhancements to certain enforcement provisions in the SFO, which would have wide-reaching implications for a regulated person's liability for misconduct and the scope of insider dealing offences. The SFC has also urged investors to be extremely careful if they intend to invest in stock tokens offered on unregulated trading platforms, and affirmed that they will not hesitate to take enforcement action against unlicensed platform operators where appropriate.

For listed companies, HKEX's enforcement actions from late 2021 to mid-2022 have focused on failures to provide proper disclosure and obtain shareholder approval.

Law reforms that impact corporate criminal liability

The SFC continues to advocate for, and seeks to expand its regulatory oversight of, the cryptocurrency sector.

The Anti-Money Laundering and Terrorist Financing Ordinance (**AMLO**) has been amended to introduce a licensing regime for virtual asset service providers (**VASP**). Unlicensed persons who, without reasonable excuse, carry on a business that is a VASP, or holds themselves out as carrying on such business, will be liable for an offence. In addition, the VASP regime has also criminalised a broad range of crypto-related misconduct, regardless of whether it takes place on a licensed VASP exchange. Offences include breach of regulations regarding the issuance of advertisements relating to virtual asset services, the use of fraudulent or deceptive devices in transactions involving virtual assets, and the use of fraudulent or reckless misrepresentations with the intention to induce investment in virtual assets. Importantly, the offences of making fraudulent or reckless misrepresentations or employing deceptive or fraudulent devices will capture all individuals and/or firms engaging in this type of conduct with a substantial nexus to Hong Kong – it is not necessary that they be physically present in Hong Kong.

Finally, in the case of non-compliance with statutory anti-money laundering and counter-terrorist financing, both the licensed VASP and its responsible officers (**ROs**) will be liable to a fine of HKD1m and two years' imprisonment upon conviction, and subject to a range of disciplinary sanctions, including revocation of the VASP licences. Corporations that wish to carry on a business that is a VASP should take careful note of the new requirements.

It is expected that the relevant legislative change will take effect in early 2023. For more details, see Regulatory roadmap for a brave and ambitious Year of the Tiger.

There will continue to be a focus on the ambit and scope of money laundering obligations in Hong Kong following the government's report in which it identified the need to enhance the AML/CFT legal framework. Money laundering obligations have been extended by amending the definition of politically exposed person (**PEP**) to include PEPs from outside Hong Kong, while changes have allowed an exemption from Enhanced Client Due Diligence (**EDD**) requirements in respect of former PEPs where the risks of money laundering and terrorist financing are low.

Corporates and their responsible officers should be made aware that the Hong Kong government has made clear their commitment to enhancing cybercrime laws and sanctions in Hong Kong. A Consultation Paper on Cyber-Dependent Crimes and Jurisdictional Issues published on 20 July 2022 included recommendations for the creation of five new cybercrime offences: (i) illegal access to programmes or data; (ii) illegal interception of computer data; (iii) illegal interference in computer data; (iv) illegal interference in computer systems; and (v) making available or possessing a device or data for committing a crime. The five new offences, if enacted, would provide penalties of up to life imprisonment, reflecting a conclusion that existing punishments are too weak to safeguard national security.

There is no proposal to create a separate legislative basis so far as concerns personal liability. The Criminal Procedure Ordinance already extends liability to directors and officers of a company if it is proven that the offence in question was committed with the consent or connivance of such person. Further consideration may be given as to whether express provision on the liability of directors and persons in a managerial capacity is needed if the present recommendations are accepted.

The proposals were open for public consultation until 19 October 2022. See A guide to Hong Kong's cybersecurity laws and practices.

Internal investigations – key developments

HKEX has published a Guidance Note on Cooperation and a revised enforcement sanctions statement. The guidance sets out examples of what may constitute good cooperation in terms of internal investigations, such as the disclosure of information not specifically requested or information that would not otherwise have been discovered by HKEX, the possible benefits of cooperation, and what may be construed as uncooperative conduct, such as late production of submissions or evidence. Importantly, cooperation includes voluntarily providing information regarding any weaknesses, failings or breaches. Meanwhile, revisions to HKEX's Sanctions Statement provide clarity on the regulator's expectations in respect of a listed issuer's internal controls and the extent to which an individual may rely on others in the discharge of their duties.

Following the consultation conclusions on the proposed Mandatory Reference Checking Scheme (**MRC Scheme**) last year, formal Guidelines on the MRC Scheme were issued in May 2022. The MRC Scheme seeks to address "rolling bad apples" in the banking sector.

Institutions recruiting for certain specified positions that fall within scope are now required to approach the former and current employer(s) of a prospective employee to request conduct-related information covering seven years prior to the application for employment. This information is expansive. It includes any breach of legal or regulatory requirements, incidents that cast doubt on an individual's honesty and integrity, internal or external disciplinary actions, and ongoing investigations. Authorised Institutions will therefore need to consider carefully how to respond to reference requests, especially while investigations are ongoing, and maintain sufficient internal employee disciplinary records on an ongoing basis so that they can easily provide the information requested.

Authorised Institutions are expected to implement Phase 1 of the MRC Scheme by May 2023. For more detail see: Hong Kong's proposed Mandatory Reference Checking Scheme: the end of "rolling bad apples"?

Sectors targeted by law reforms or enforcement action

The SFC's investigations have continued to focus on intermediary misconduct and corporate misconduct, including keeping a close watch on internal control deficiencies, sponsors' due diligence failures and mis-selling of financial products.

The HKEX's enforcement actions in 2022 against listed corporations and/or its senior management have been in a mix of industry sectors. Those include property development, renewable energy, telecommunications, advertising and food and beverages. The focus was on the maintenance of adequate and effective systems and internal controls to ensure an issuer's and the company directors' compliance with their obligations.

In 2022, we saw the first criminal prosecution for market misconduct of a former senior manager at a crypto exchange; the senior manager was accused of illicitly making HKD5m by secretly trading against the company. The senior manager was charged with accessing the company's internal systems "with criminal or dishonest intent" by setting up a retail account in his father's name and trading against a corporate account he controlled, making a profit of about HKD5m in the form of USDT, the crypto industry's largest stablecoin.

The Competition Commission is focused on investigations and bringing enforcement action where appropriate in the digital sector, having recently imposed sanctions on two competing travel services over a price-fixing cartel case.

Cross-border cooperation investigation or enforcement activity

There has been a slight increase in enforcement-related cross-border requests received and made by the SFC in 2020/2021 compared to the previous year. This trend will likely intensify given increased enforcement activity in a number of jurisdictions arising from recent macro-economic developments and other issues.

Meanwhile, the SFC maintained close enforcement cooperation with the China Securities Regulatory Commission (**CSRC**). In particular, the SFC held a meeting with the CSRC in June 2022 to discuss their enforcement cooperation efforts, and agreed on follow-up arrangements for emerging issues related to cross-boundary enforcement cooperation issues.

December 2021 saw a joint operation between regulators and law enforcement agencies in Singapore and Hong Kong to protect the integrity of the securities markets. The SFC, the HKPF, the Monetary Authority of Singapore (**MAS**) and the Singapore Police Force (**Singapore Police**) announced that they had conducted a joint operation against an active and sophisticated syndicate suspected of operating ramp-and-dump manipulation schemes. Ten individuals believed to be the key members of the syndicate, their associates and some senior executives of Hong Kong-listed companies were arrested during searches of 33 premises in Hong Kong and Singapore by more than 190 officers of the SFC, the HKPF, the MAS and the Singapore Police. A joint operation on this scale was unprecedented.

The SFC continues to agree memoranda of understanding (**MoU**) guidelines with various local and international regulators in order to aid future cooperation and to enhance cooperation and the exchange of information, including an MoU with the European Securities and Markets Authority, the EU's financial markets regulator and supervisor, and a joint circular with the Australian Securities and Investments Commission on their collaborative thematic review of global financial institutions' foreign exchange businesses and operations in Hong Kong and Australia.

Similarly, the Personal Data authorities in Hong Kong and Singapore renewed an MoU to maintain their existing ties and foster closer cooperation with an enhanced scope of collaboration in personal data protection. See the PCPD's media statement here.

Predictions for 2023

An increase in collaboration between regulators

We expect to see an increase in collaboration between local regulators in Hong Kong, such as the SFC and the ICAC, by conducting joint operations to combat corporate fraud and misconduct of listed companies, directors or shareholders.

Continued efforts to bring the cryptocurrency markets within the purview of regulators

Historically, the SFC's regulatory approach was to only allow professional investors to invest in Virtual Asset (**VA**)-related funds and securities offered in Hong Kong. However, in November 2022, the SFC announced that Hong Kong intends to make significant moves toward a more open and inclusive approach to VA-related investments in order to foster the sustainable development of a vibrant ecosystem for VAs. Specifically, the SFC plans on opening up access to virtual asset investments for the retail market.

The SFC has also issued a Circular on the requirements for seeking SFC authorisation for public offerings in Hong Kong of exchange traded funds (**ETFs**). The SFC has stated that it is prepared to accept applications for authorisation of VA Futures ETFs traded on traditional regulated futures exchanges.

Key team members

Matt Bower
Partner – Hong Kong
Tel +852 2974 7131
matt.bower@allenovery.com

Fai Hung Cheung
Partner – Hong Kong
Tel +852 2974 7207
fai.hung.cheung@allenovery.com

"Hugely experienced disputes team with a distinguished track record acting for high-profile banking and corporate clients on contentious matters…. Also offers expertise in regulatory investigations and mis-selling claims, leveraging the strength of the firm's fraud, white-collar crime and money-laundering practices. Particularly noted for its work on multi-jurisdictional disputes across the Asia-Pacific region."

Chambers Asia-Pacific Guide, 2021 – China, Dispute Resolution: Litigation

"Offers a strong contentious offering, including handling high-profile SFC and CSRC investigations."

Chambers Asia-Pacific Guide, 2021 – China, Financial Services

"Allen & Overy garners praise for its 'deep understanding of the regulatory landscape'… Matt Bower has expertise in acting for financial institutions in regulatory investigations."

Legal 500 Asia Pacific, 2021 – Hong Kong, Regulatory

Netherlands

The past year has seen a vast increase in attention paid to sanctions legislation due to the ongoing war in Ukraine. Investigations into non-compliance with Anti-Money Laundering regulations also remain a high priority for Dutch enforcement authorities.
In addition, the Dutch Public Prosecution Service (DPPS) continues to focus on the prosecution of individuals, in cases where a legal entity enters a settlement with the DPPS.
We expect increased scrutiny of tax integrity, cybercrime and business responsibility for human rights in 2023.

Investigation trends/developments

Corporate crime defence

The DPPS remains focused on the criminal liability of individuals following high value settlements with legal entities. Implicated individuals are not automatically included in such settlements. The DPPS adheres to its 'Instruction on High-Value Settlements' which prescribes that implicated individuals will be prosecuted if possible. Each case will be judged on its own merits in connection with the DPPS's decision to prosecute. For example, four former board members of a financial institution were recently identified as suspects in an ongoing investigation, while that financial institution reached a large settlement in the same case two years ago.

Anti-bribery and corruption

In July 2022, the DPPS issued its Instruction on the Investigation and Prosecution of Domestic Official Bribery which shows a renewed focus on the investigation and prosecution of bribery of domestic public officials. Although the Instruction relates to domestic bribery, it is expected that the focus on bribery of foreign officials will also increase.

Mediation and negotiated justice in criminal cases

Mediation plays an increasingly significant role in the Netherlands, including in criminal cases. As of 1 January 2023, the Dutch Criminal Code contains a new provision for a criminal case to be referred to mediation by a prosecutor or judge as part of a three year pilot for such mediation.

There is a particular willingness to engage in mediation by the Dutch tax authorities, and we therefore also expect to see this in tax fraud enforcement. Mediation helps foster a constructive relationship between the Dutch tax authorities and the parties involved after the settlement of the dispute.

'Negotiated justice' is another trend, involving an agreement between the prosecution and the defendant, such as a lower sentencing demand by the prosecutor, in exchange for a guilty plea. Although such agreements do not have a legal basis, they seem to be gradually accepted by different courts.

Other enforcement instruments

The DPPS used its inquiry power in a recent civil case after a miscreant former board member was reinstated as managing director in an IT company which provides services to the Dutch government. The right of inquiry is a form of dispute resolution in which interested parties request a special enterprise chamber of the court to investigate a company. The objectives of an inquiry procedure are remediation, the restoration of healthy relations within the company, opening up matters and determining who is responsible for possible mismanagement. In the right of inquiry, the interests of the enterprise driven by the company are the central focus. The DPPS rarely uses this power, which makes it striking that it has chosen to do so now. We are curious whether the DPPS will use this power more often when ESG issues are at stake.

Significant law reforms impacting corporate criminal liability

Corporate criminal liability

The government's 'Money Laundering Action Plan' proposes that an institution should, under certain conditions, take reasonable steps to investigate whether another institution has provided or refused services to certain high-risk clients, to prevent customers from 'shopping around' for an institution.

The requirement to register Ultimate Beneficial Owners (**UBO**) of trusts recently entered into force. UBOs of trusts must be registered before 1 February 2023. The UBO register currently cannot be accessed by the general public following a judgement by the Court of Justice of the EU about the access to the (Luxembourg) UBO register violating the right to privacy. Despite this, the obligations under the Dutch AML Act remain applicable, including the obligation to obtain proof of registration of UBOs in the register.

In 2022, the Dutch Child Labour Due Diligence Act was expected to come into force requiring companies that have a reasonable suspicion that child labour may be involved in their manufacturing process to develop and implement action plans to address these risks. Instead, the Dutch government will strive to incorporate this Act as part of broader EU legislation on international responsible business conduct.

International sanctions

The war in Ukraine has led to an unprecedented array of adopted sanctions in the EU. There has been an increase in the number of investigations for sanctions violations, with a focus on asset freezes and circumvention of sanctions. Supervision is also focused on the use of dual-use goods and unusual transactions to fall-back countries such as Kazakhstan. As a result, sanctions are a trending topic in many sectors and companies must remain vigilant around sanctions legislation. We expect a growing focus on sanction enforcement in the coming year.

Cybercrime

Cybercrime has been growing exponentially over the past few years. Moreover, the DPPS is noticing an increase in the fusion of more traditional crimes and cybercrime. To effectively counter cybercrime, the Dutch Ministry of Justice and Security recently implemented a two-track system. The first track focuses on prevention of cybercrime and limiting the impact of cybercrime on victims. The second track focuses on investigation, prosecution and disruption. The prevention of cybercrime and the incorporation of a cyber-defence policy is a priority on an EU level too. A new proposed EU regulation aims to increase the cybersecurity resilience of EU Member States. The new legislation sets stricter requirements for companies, governments and infrastructure, and covers new "essential sectors" such as energy, transport, banking and health.

Whistleblower directive – implementation in Dutch law

The Dutch law to implement the 2019 EU whistleblowing directive was adopted on 20 December 2022. Whistleblowing was already partially regulated under Dutch law, but the newly adopted law has a broader scope. Under certain conditions, the Whistleblower Authority will be able to impose sanctions on employers through administrative law. The Whistleblower Authority may impose sanctions if the employer does not behave properly towards the whistleblower, does not follow up on the recommendations of the investigation department or has not set up a proper internal reporting channel.

In addition, employers are obliged to designate independent officials to whom a report can anonymously be made in their reporting procedure. This independent officer must have certified training, take an oath, and cannot work for the company. A lawyer is mentioned as an example of an independent officer. The law is expected to enter into force on 1 July 2023.

Internal investigations – key developments

Lawyers and internal investigations

We increasingly see cross-border internal investigations into sexual misconduct in the workplace, environmental fraud or greenwashing, or social fraud. The general council of the Dutch Bar Association (*Nederlandse Orde van Advocaten*, **NOvA**) previously clarified the code of conduct for lawyers involved in internal investigations by stating that lawyers can carry out internal investigations without breaching professional conduct rules.

In July 2022, the NOvA's Disciplinary Board ruled that internal investigations intended for external use must meet certain conditions. It is beyond dispute that a lawyer can have a role as a fact-finding investigator in the interest of the client. The Disciplinary Board seems to be adding a role to this, as it rules that lawyers can act as independent investigators too.

There is still some ambiguity surrounding the role of the internal investigator. For the majority of lawyers, who use fact-finding for their core task, namely to advise their clients on their legal position and to assist them in legal disputes, this ruling hardly changes anything. They will continue to be able to use fact-finding as an integral part of their duties.

Legal privilege

The scope of legal privilege in tax matters in the Netherlands was a hotly debated topic. A draft bill proposed that the legal privilege of lawyers and civil-law notaries would only cover information that is directly linked to a lawyer's activities aimed at the determination of the legal position, representation and defence of their clients and advice before, during and after legal proceedings. The draft bill was met with criticism, including from the Dutch Bar Association and the Royal Notarial Association. Subsequently, the draft bill was amended and the current draft will not affect the lawyer's legal privilege.

Sectors targeted by law reforms or enforcement action

As we predicted last year, the Dutch Central Bank (the **DNB**) has started imposing fines on exchange services between virtual and fiat currencies and custodial wallet providers for not complying with the registration requirement under the AML Act. The DNB will continue to closely monitor both registered providers as well as foreign providers without registration. Acting in breach of the registration requirement is a criminal offence under the Economic Offences Act (*Wet op de Economische Delicten*). The DNB focuses on institutions more recently placed under their supervision like audit firms and payment service providers, in addition to the focus on traditional financial institutions.

Performing customer due diligence, unusual transaction reporting, and complying with other AML rules properly are vital responsibilities that the DNB monitors closely. There is, however, some room for innovation: a recent court ruling permitted the use of artificial intelligence as an aid for certain customer due diligence obligations under AML regulations.

DNB and the DPPS also work together for enforcement purposes. DNB notified the DPPS of potential breaches of the Dutch AML Act within a Dutch financial institution, and the DPPS recently announced it is investigating those alleged breaches. Prior to this investigation, two other Dutch financial institutions already negotiated large out-of-court settlements for culpable money laundering.

Cross-border coordinated enforcement activity

The EPPO has opened more than 4000 investigations across the EU since commencing its work in June 2021. One ongoing complex investigation into EUR2.2bn worth of VAT fraud is currently active in 14 EU Member States, including the Netherlands.

Predictions for 2023

– We expect the Dutch enforcement authorities to have a growing focus on the financial sector, including traditional institutions (banks) as well as new participants such as crypto exchanges and electronic money institutions. Moreover, we expect more investigations into corruption.

– The Ministry of Finance has asked citizens and businesses to report conspicuous tax arrangements 'that comply with the letter of the law, but not with its spirit'. Reports can be made until the end of January 2023. After that, these reports will be investigated. In general, we expect an increased focus on tax integrity issues.

– The extensive EU sanctions package against Russia has led to a desire to renew the Sanctions Act, the Dutch legislation on the enforcement of sanctions violations. A draft bill for the modernisation is expected in the course of 2023.

– A bill is being drafted (Confiscation of Criminal Assets Bill) to enable the DPPS to confiscate criminally acquired assets without a criminal conviction (non-conviction based confiscation).

– We expect that the Dutch Parliament will start deliberations on the proposal for the judicial review of high transaction settlements. An independent Review Committee currently undertakes this review. At present, the Dutch Code of Criminal Procedure is being modernised. This modernisation includes the replacement of the Review Committee by a judicial review.

Key team members

Hendrik Jan Biemond
Partner – Netherlands
Tel +31 20 674 1876
hendrikjan.biemond@allenovery.com

Patrick Ploeger
Partner – Netherlands
+31 20 674 1336
patrick.ploeger@allenovery.com

Kim Helwegen
Senior Associate – Netherlands
Tel + 31 20 674 1613
kim.helwegen@allenovery.com

Irem Çakir
Associate – Netherlands
Tel +31 20 674 1758
irem.cakir@allenovery.com

Iris van den Oord
Associate – Netherlands
Tel +31 20 674 1585
iris.vandenoord@allenovery.com

"Hendrik Jan Biemond leads a very good team with complementary strengths."

The Legal 500, 2022 – Fraud and White-Collar Crime

"Allen & Overy is very knowledgeable, both from a legal content point of view, but also in practical ways: what to expect when and how to act."

Chambers Europe, 2022 – White-Collar Crime & Corporate Investigations

"Low barrier to communication and very easy to approach, with clear out-of-the-box thinking."

The Legal 500, 2022 – Fraud and White-Collar Crime

South Africa

The risk of the Financial Action Task Force (**FATF**) greylisting looms large over recent South African reforms, as do the ongoing consequences of "state capture". The four-year-long Judicial Commission of Enquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector including Organs of State (**Zondo Commission**) has submitted its final report to the President. The Presidency, Parliament, law enforcement and regulators have shifted to pursuing criminal prosecutions and administrative penalties against offenders, recovering funds and considering necessary legislative and institutional reforms. High-profile arrests and settlement agreements relating to state capture and asset-freezing related to corporate accounting and reporting fraud have dominated the latter part of 2022. We anticipate that 2023 is likely to see similar arrests, extensive litigation and a raft of legislative reform focused on preventing money-laundering and regulating public procurement. State capture investigations have prompted increasing cooperation between law enforcement and regulatory agencies which has extended to using relatively powerful anti-money laundering (**AML**), tax evasion and exchange control remedies to combat corporate fraud as well as environmental and cyber-crimes.

Investigations trends/developments

State Capture Commission concludes

The Zondo Commission, initiated in January 2018, submitted the final volume of its report in June 2022. Its over 350 recommendations include referrals to investigatory and prosecution authorities, asset-recovery and disciplinary sanction by professional bodies as well as legislative, constitutional and institutional reforms. A National Anti-Corruption Advisory Council, appointed by the President in August 2022, has contributed to the President's formal response and may become a permanent feature of the anti-corruption framework. The President has committed to considering various reforms including legislative amendments to strengthen NPA independence; increased private sector obligations when dealing with the State; improved whistleblower protections; and finalisation of the long-delayed Public Procurement Bill.

Regulators ramp up

As the Special Investigating Unit (**SIU**) continues its investigations, an increasing number of civil recovery proceedings, administrative reviews and asset-freezing applications are being brought before the Special Tribunal and High Courts. The results of the joint "state capture" task force of the NPA and Directorate for Priority Crime Investigation are starting to be seen with a pattern of charging former state officials, together with implicated private individuals and companies. In addition to NPA collaborations with the South African Revenue Service (**SARS**), Financial Intelligence Centre (**FIC**) and South African Reserve Bank (**SARB**), the Companies and Intellectual Property Commission (**CIPC**) has commenced compliance reviews of implicated companies. Black-listing has also been mooted, with the National Treasury imposing a ten-year ban from tendering for public sector contracts on a large management consulting firm in September 2022 and stating that it, together with SARS, is considering restricting the firm's directors.

Public procurement under the spotlight

Public entities, state departments and the SIU have launched increasing numbers of "self-review" applications to have unlawful conduct set aside and recover funds from private companies involved in procurement irregularities, fraud and corruption. The result has been rapidly developing precedent regarding principles of public procurement, consequences of unlawful public contracts and the due diligence obligations of private parties contracting with the state. In parallel, high-profile settlement agreements have continued, including the Department of Water and Sanitation's settlements with two foreign IT companies for approximately ZAR177m and ZAR345m respectively. Settlement agreements concluded in previous years, however, have not deterred authorities from pursuing criminal sanctions against implicated individuals, as evidenced by arrests and charges against company representatives implicated in the Kusile power station and Transnet locomotive cases.

Freezing, forfeiture and insolvencies

A trend, extending beyond state capture cases, is the authorities' use of asset-freezing and forfeiture provisions targeting the proceeds of financial and environmental crime. Asset Forfeiture Unit (**AFU**) confiscation orders include those relating to proceeds of abalone poaching while the largest cumulative preservation order obtained by the AFU to date is linked to the Gupta family's Optimum Coal Mine and Coal Terminal assets (estimated to be in excess of ZAR8bn).

The SIU has obtained preservation orders against bank accounts, properties and pension benefits of a range of state capture-implicated individuals and companies. While frozen assets have been placed under curatorship, in some cases, insolvency proceedings are also underway. In some cases, asset forfeiture and insolvency proceedings have been at the instance of the SARS and the SARB. The SARB's attachment of assets belonging to a former CEO of a large global retailer rests on the powerful penalty provisions in the Exchange Control Regulations. These allow for the forfeiture of the contravention amount to the state as well as a fine of the larger of ZAR250,000 or the contravention amount (and/or imprisonment of up to five years). In this case, contraventions are estimated at ZA 4.835bn with the court also ordering the appointment of forensic experts and a supervising attorney to evaluate assets and uplift material relevant to the SARB's investigations. Similarly, the SARS' focus on the tobacco, gold and fuel industries has led to provisions in the Tax Administration Act being used to place assets of Gold Leaf Tobacco Corporation and its directors under curatorship.

Significant law reforms impacting corporate criminal liability

Greylisting risk and focus on beneficial ownership

The Financial Action Task Force's threat of 'greylisting' South Africa has generated a number of amendment bills and directives from the Prudential Authority on beneficial ownership reporting, enhanced customer due diligence requirements, and criminal background checks on directors and officers.

New General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act includes amendments to South Africa's financial sector regulatory framework legislation and the regulation of trusts, Non-profit Organisations (**NPOs**) and companies to enhance oversight and reporting over beneficial ownership. Its amendments to the Trust Property Control Act, 57 of 1988, Nonprofit Organisation Act, 71 of 1997 and Companies Act, 71 of 2008 include requirements for collection, retention and reporting of beneficial ownership information and contemplate access to beneficial ownership information in the respective registers of the Masters Office, NPO Directorate and CIPC. Registration of NPOs making donations or providing services outside of South Africa is to become mandatory with offences for registration failures and non-compliance with disclosure requirements. There would be increased fines of up to ZAR10m and/or five years' imprisonment for non-disclosures by trustees.

Expanded KYC obligations and disqualification requirements

Amendments to the Financial Intelligence Centre Act, 38 of 2001 (**FICA**) and the Financial Sector Regulation Act, 9 of 2017 include KYC requirements for trustees, trust beneficiaries and partnerships; draw the estate agency and gambling sectors within scope; and increase accountable institutions' risk management obligations regarding new and existing clients. The Prudential Authority's directive, requiring enhanced due diligence and criminal background checks on directors and senior officers of entities subject to the Banks Act, 94 of 1990, anticipates these more stringent KYC requirements, powers of regulators to issue minimum standards for KYC reporting by beneficial owners and financial institutions and an expansion of disqualification requirements for trustees, NPO officers and company directors.

Proliferation financing and sanctions

Responding to FATF recommendations, the Prudential Authority has provided a Guidance Note to the banking sector on how to identify and assess proliferation finance risks. The FICA amendments expand its scope to include proliferation financing activities and the range of persons required to freeze assets under UN sanctions. Amendments contemplate the automatic effectiveness of UN Financial Sanctions, under Chapter VII of the UN Charter, without the need for Ministerial gazetting. Amendments also include empowering the FIC to provide forensic evidence for the purposes of court proceedings and for administrative penalties for non-compliance (in addition to existing criminal sanctions).

Internal investigations – key considerations

Access to information requests and privilege

The number of complex investigations linked to state capture and high-profile corporate frauds has placed increasing pressure on corporates to release internal investigations reports to the media and regulators. Two of South Africa's prominent investigative news outlets have successfully obtained a May 2022 court order to access a forensic accounting report commissioned by a major global retailer through its attorneys. The press argued that any privilege claimed over the report was limited by the media's right to receive and impart information or ideas. The court's decision ultimately turned on a factual finding that the company had waived its privilege. While we understand the order is subject to appeal, the judgment has been hailed by the press and civil society as a victory for media freedom and the role of the press in ensuring corporate transparency. The court's approach provides a cautionary tale regarding protecting privilege and exercising vigilance in the publication of investigation outcomes balanced against their regulatory reporting obligations.

The public interest and personal information

An area to watch is how personal information is managed and the basis on which it may be disclosed to regulators or in the public interest. The Information Regulator has approved codes of conduct for processing personal information by South Africa's Banking and Credit Bureau Associations while launching its Enforcement Division during the course of 2022. It is not yet clear whether the joint oversight by the Information Regulator over the Protection of Personal Information Act, 4 of 2013 (**POPIA**) and the Promotion of Access to Information Act, 3 of 2000 will assist in how these statutes intersect. A recent High Court analysis suggests that access to information may be ordered to protect the public interest where personal information has already been submitted to regulators, in this case privacy rights limited by the public interest in information regarding the permitting of leopard hunting.

Sectors targeted by law reforms or enforcement action

Financial services sector and auditing profession

While enforcement action has focused on state-owned enterprises, complex fraud and money-laundering through public-private partnerships and tender fraud, the conduct of auditors and accurate financial reporting have also been targeted. An important trend is financial services regulators and the SARS focusing on corporate adherence to customer risk assessments and compliance with prudential standards. Sanctions imposed by the FSCA under FICA in the 2021/2022 financial year all related to defective Risk Management and Compliance Programmes, failure to conduct Customer Due Diligence or failure to file Cash Threshold Reports with financial penalties ranging from R20,000 to R6.3m.

The beginnings of crypto-regulation?

After a two-year period of public comment and consideration, the FSCA has declared crypto assets as "Financial Products" under the Financial and Intermediary Services Act, 2002, publishing a policy document supporting the declaration and announcing a licensing period between June and November 2023. This appears to be the first step in drawing crypto asset service providers and crypto exchanges within the financial regulatory framework.

Cross-border coordination investigation or enforcement activity

A continuing trend is coordinated cross-border investigation and enforcement relating to cyber- and environmental crime, both linked to international money-laundering networks.

Cybercrime and extraditions

South Africa has been part of ongoing INTERPOL coordinated action against members of the cyber-fraud gang, Black Axe, and related groups. The most recently announced arrests include two suspects in South Africa linked to online scams while extradition requests from the U.S. in relation to previous arrests are subject to court review. South Africa's own requests for international cooperation include extradition requests linked to high-profile corporate crime, including the Gupta brothers (wanted in connection with state capture-related charges) and persons implicated in a multi-jurisdictional accounting fraud of a listed company, a ZAR745m corruption case involving Eskom and the 2020 bitcoin-based Ponzi scheme linked to Mirror Trading International.

Money-laundering and tax offences expose wildlife crime

A number of multi-agency and cross-border operations have focused on exposing wildlife crime through tax investigations and suspicious transaction reports. One such operation included the SARS together with agencies such as the wildlife divisions of the DPCI and South African Police Service, South African National Parks, the Department of Environmental Affairs and the AFU arresting members of an international syndicate involved in rhino-horn trafficking which was exposed through tax evasion. Inter-agency cooperation to prevent wildlife crime more broadly includes the FIC, DFFE and the public-private partnership, the South African Anti-Money-Laundering Integrated Task Force.

Predictions for 2023

FATF response and State Capture repercussions

2023 is likely to be dominated by legislative and regulatory reform prompted by South Africa's need to respond to the FATF recommendations and political pressure to see results from the Zondo Commission. While some of the more controversial legislative reforms may remain subject to legal challenge, regulators are currently using existing powers to issue directives and guidance to impose greater reporting and due diligence obligations on the financial services sector. Criminal proceedings against those involved in state capture may lead to additional investigations by regulators and investigatory authorities, including calling upon third parties to provide evidence and the need for in-house legal teams to manage competing information requests.
It is also possible that banking, insurance, auditing and legal possession may come under greater scrutiny in terms of obligations to monitor and report suspicions of unlawful activity.

Tax and AML disclosures to tackle organised crime

The approach of regulators and the National Prosecuting Authority (NPA) to organised crime has increasingly turned to the relatively powerful AML and tax regimes. For example, the NPA has pursued money laundering charges against those arrested for illegal mining or possession, disposal and transportation of minerals due to the more stringent sentences available for money laundering offences. Similarly, the SARS has focused on pursuing VAT carousels in tackling illegality in the secondary gold market. The relatively powerful tools of tax audits and money laundering reporting obligations are likely to continue to be used to investigate organised crime, complex corporate fraud and cross-border criminal activity with investigatory authorities relying on information gathered from corporate and financial services reporting.

Key team members

Gerhard Rudolph
Partner – Johannesburg
Tel +31 653 889 291
gerhard.rudolph@allenovery.com

Callum O'Connor
Counsel – Johannesburg
Tel +31 682 359 843
callum.oconnor@allenovery.com

Nina Braude
Senior Associate – Johannesburg
Tel +27 10 597 9921
nina.braude@allenovery.com

"Gerhard [Rudolph] is a seasoned litigator having been involved in many pieces of sophisticated litigation over the years. He has been both articulate and creative in the handling of matters."

Chambers, 2022 – South Africa, Dispute Resolution

"Callum O'Connor is always accessible and demonstrates sound legal advice within a business context."

Chambers Global Guide, 2022 – South Africa, Corporate Investigations

"Excellent international and cross-border capability; well-resourced and thorough; thoughtful and collaborative."

Legal 500 Global-wide, 2022 – Corporate Investigations and White-Collar Criminal Defense

"The team evaluates information from all possible angles and determines the risks that come with various approaches."

Legal 500 Global-wide, 2022 – Corporate Investigations and White-Collar Criminal Defense

United Arab Emirates

2022 was another busy year for the UAE as it seeks to further develop its regulatory framework. The UAE continued with significant regulatory development and expansion, including in the areas of anti-money laundering (**AML**)/counter-terrorist financing (**CTF**) compliance, whistleblowing, data protection and virtual assets. These developments continue to have implications for both the UAE's onshore jurisdiction and its offshore jurisdictions, including the Dubai International Financial Centre (**DIFC**) and the Abu Dhabi Global Market (**ADGM**).

We expect to see the UAE authorities place a greater focus on monitoring and enforcing compliance with new and existing regimes in the year ahead. Businesses should therefore take prompt and proactive steps to ensure they are compliant with all regimes applicable to them so that monitoring and enforcement risks on the horizon can be appropriately managed and mitigated.

Investigations trends/developments

AML a prominent area of focus

AML is a prominent area of focus for law reform and the authorities in the UAE, in part due to pressure from the Financial Action Task Force (FATF), an intergovernmental organisation aimed at tackling money laundering.

In early 2022, the FATF placed the UAE on its 'grey list' of jurisdictions and under enhanced monitoring due to "strategic deficiencies" in its efforts to counter money laundering and terrorist financing. Removal from the grey list requires the UAE to fully implement the recommendations set out in the FATF's action plan that was issued following the FATF's 2020 Mutual Evaluation of the UAE.

The FATF has acknowledged that the UAE has made significant progress, addressing more than half of the key actions recommended by the FATF in 2020. The remaining actions which the UAE is focused on progressing to fully implement the plan include:

- demonstrating through case studies and statistics a sustained increase in outbound Mutual Legal Assistance requests to help facilitate investigation of terrorist financing (**TF**), money laundering (**ML**), and high-risk predicates
- identifying and maintaining a shared understanding of the ML/TF risks between the different Designated Non-Financial Businesses and Professions (**DNFBPs**) sectors and institutions

– showing an increase in the number and quality of Suspicious Transaction Reports filed by financial institutions and DNFBPs

– achieving a more granular understanding of the risk of abuse of legal persons and, where applicable, legal arrangements, for money laundering/terrorist financing

– providing additional resources to the Financial Intelligence Unit to strengthen its analysis function and enhance the use of financial intelligence to pursue high-risk money laundering threats, such as proceeds of foreign predicate offences, trade-based money laundering, and third party laundering

– demonstrating a sustained increase in effective investigations and prosecutions of different types of money laundering cases consistent with the UAE's risk profile

– proactively identifying and combating sanctions evasion, including by using detailed targeted financial sanctions guidance in sustained awareness-raising with the private sector and demonstrating a better understanding of sanctions evasion among the private sector.

These will all be familiar features of AML regimes under which many companies already operate.

Politically Exposed Persons (PEPs) under scrutiny from the Central Bank

The Central Bank of the UAE issued new guidance on AML and CTF, specifically in relation to PEPs. The guidance makes clear that licensed financial institutions must:

– develop risk-based policies to ensure they appropriately identify PEPs or related customers prior to on-boarding

– obtain senior approval before establishing a business relationship with a foreign PEP

– take reasonable measures to establish the source of funds and source of wealth for foreign PEPs

– apply a risk rating to the PEP which takes into account factors such as the nature of the PEP's position, and the controls in place in the PEP's jurisdiction to prevent corruption

– conduct ongoing monitoring of the business relationship

– maintain transaction monitoring systems equipped to identify patterns of unusual or suspicious activity

– file a suspicious transaction/activity report with the Financial Intelligence Unit where there are reasonable grounds to suspect a transaction, attempted transaction, or funds constitute the proceeds of crime, are related to a crime, or are intended to be used in a crime.

New whistleblowing regimes aim to encourage more disclosures

A number of enhancements have been made to improve whistleblower protections in the UAE. We expect these enhancements to lead to an increase in reporting both internally and externally, and to a corresponding increase in investigations, as they become embedded and awareness about them is raised in the market:

The Dubai Financial Services Authority (**DFSA**) introduced its new whistleblowing regime in April 2022, which strengthens protections available to whistleblowers making disclosures in respect of DFSA-regulated entities.

The Abu Dhabi Accountability Authority (**ADAA**), the independent Abu Dhabi government authority with oversight of all Abu Dhabi government departments and agencies and corporate entities which are wholly or partially owned by the Abu Dhabi State, launched the "Wajib" platform, which allows confidential reports of financial and administrative corruption to be made in respect of entities under the supervision of the ADAA. ADAA expects reports of abuse of power, misappropriation of funds, manipulation of financial statements and any other financial or administrative corruption.

More data protection investigations likely

While the new UAE Data Office (which has been established to oversee a new Federal Data Protection Law) is not yet fully operational, it will have the power to conduct investigations to ensure compliance with new data privacy legislation (see below). The regulator will have the power to fine organisations for non-compliance.

Significant law reforms impacting corporate criminal liability

New data protection laws

A new Federal Data Protection Law, which came into force on 2 January 2022, applies to: an individual who resides or has a place of business in the UAE; an organisation that is established in the UAE that processes the Personal Data of individuals, whether those individuals are located inside or outside the UAE; and an organisation that is not established in the UAE but that processes the Personal Data of individuals that are located inside the UAE.

The Data Protection Law does not apply to public entities or entities based in the UAE's free zones, a number of which (including the DIFC and the ADGM) have their own data protection laws in place. The Data Protection Law also does not apply to health or credit data that is governed by existing sectoral legislation.

The Data Protection Law is closely modelled on the EU's data protection regime, but notably, the UAE has not included a 'legitimate interest' basis for processing Personal Data. As a result, the primary lawful basis on which organisations may process Personal Data remains consent, though there are limited exceptions to the requirement to obtain an individual's consent, such as processing which is necessary for the performance of a contract to which the individual is a party, or processing required for the defence of a legal claim. The Data Protection Law introduces many concepts into UAE law for the first time that are similar to the equivalent terms used in the GDPR, ADGM and DIFC data protection laws. These include well-established principles, such as the requirement for the processing of Personal Data to be fair, transparent and lawful.

Virtual assets regulation

Combatting financial crime is a core driver of the continuing reforms in the virtual assets sector due to the heightened AML and CTF risks that these products attract. Listen to our podcast on the developing virtual asset landscape in the UAE and its interaction with AML and CTF considerations here. Developments in this area include:

A new law on virtual assets (Dubai Law No. 4 of 2022), which came into force in March 2022. It is the first law in Dubai which specifically regulates virtual assets and follows a raft of other developments in the UAE in the area of virtual asset regulation. The new law establishes the Virtual Assets Regulatory Authority (**VARA**), an independent regulatory body affiliated with the Dubai World Trade Centre which is mandated to authorise activities involving virtual assets in Dubai, including in specialist development zones and free zones (with the exception of the DIFC).

A new crypto regime overseen by the DFSA, which came into force on 1 November 2022. This builds on the introduction by the DIFC of a regime for the regulation of investment tokens in October 2021. The new regime is intended to address money laundering and terrorist financing risks in respect of trading, clearing, holding or transferring crypto tokens, as well as consumer protection considerations. Certain tokens (including NFTs) fall outside of the scope of the new regime. However, issuers of these tokens are still required to register with the DFSA as a designated non-financial business or profession (DNFBP) and comply with the AML regimes in both the UAE and the DIFC.

The DFSA will likely issue future public consultations on a wide range of crypto-related issues, such as staking and DeFI (decentralised finance), prudential rules and capital requirements in respect of crypto firms as well as more detailed guidance for the crypto industry on AML issues such as enhanced due diligence and account monitoring requirements.

Cross-border cooperation on enforcement

The UAE is taking further steps to promote cross-border cooperation. In 2022, the UAE signed mutual legal assistance treaties and international judicial cooperation agreements with the United States, Ethiopia, Denmark, Lithuania, and Serbia. These allow for greater collaboration and information sharing on criminal investigations and prosecutions.

In October 2022, the UAE's Executive Office of Anti-Money Laundering and Counter Terrorism Financing signed a memorandum of understanding with the United Nations Office on Drugs and Crime, in an effort to expand cooperation and tackle the movement of illicit funds.

The DFSA is also continuing to work closely with its global counterparts. In addition to the more than 100 bilateral and multilateral memoranda of understanding that it already has in place, the DFSA recently signed memoranda of understanding with regulators in Bangladesh, India, and Mauritius, with particular emphasis placed on mitigating ML and TF risks among supervised entities. During the past year, the DFSA received 56 regulatory requests for information and assistance from other regulators, while the DFSA made 92 requests to fellow regulators for information.

Predictions for 2023

Following the decision by FATF to place the UAE on the grey list and under increased monitoring, it is likely that the UAE will focus on demonstrating that its AML/CTF regime operates effectively in practice, including through promoting increased suspicious transaction/activity reporting from businesses and an increase in enforcement activity. Firms should continue to ensure that they place sufficient focus on, and investment in, the development of appropriate AML/CTF controls, including putting in place clear and effective policies and procedures to ensure compliance with AML/CTF regulations.

Following the introduction of the DFSA Whistleblower Regime and the introduction of the ADAA's "Wajib" platform, we expect to see the UAE take further steps to embed protections for whistleblowers and to publish guidance on how these protections should be implemented in practice. Businesses should carefully consider the requirements of the whistleblower protection regimes applicable to them and ensure that proper processes are in place to facilitate reporting and adequate protection for whistleblowers.

Businesses should consider whether their policies, procedures and operations are compliant with the requirements of the Federal Data Protection Law now that it is in force. We expect to see more activity from the UAE Data Office in the coming year as the Data Protection Law becomes embedded and the UAE authorities seek to monitor compliance with the legislation.

Consistent with global trends, both the onshore and offshore UAE jurisdictions look set to expand their activities and regulation in this area at pace. Virtual Asset Service Providers and other relevant market participants should therefore keep a close eye on regulatory developments in this area, particularly in Dubai and the DIFC, where significant further activity is anticipated.

Key team members

Yacine Francis
Partner – Dubai
Tel +971 4 426 7228
yacine.francis@allenovery.com

David Berman
Senior Associate – Dubai
Tel +971 4 426 7245
david.berman@allenovery.com

David Odejayi
Associate – Dubai
Tel +971 4 4426 7191
david.odejayi@allenovery.com

Charlotte McGing
Associate – Dubai
Tel +971 4 426 7207
charlotte.mcging@allenovery.com

Rachel Green
Associate – Dubai
Tel +971 4 426 7112
rachel.green@allenovery.com

"A highly regarded disputes department which is well acquainted with international matters."

Chambers Global, 2022 – UAE, Dispute Resolution

"An excellent firm with great technical ability."

Chambers Global, 2022 – UAE, Dispute Resolution

"They are a great team with a breadth of expertise."

Chambers Global Middle East, 2022 – Dispute Resolution

"The A&O team are a cut above the rest in terms of their commercial and technical acumen."

Legal 500 UAE, 2021 – Dispute Resolution: Arbitration and International Litigation

United Kingdom

The Russian invasion of Ukraine hastened legislative reform aimed at stemming the flow of 'dirty money' in the UK and aiding the enforcement of financial sanctions. Not so hasty is a new 'failure to prevent' economic crime offence, which is still not on the statute books. Supporters of reform will have been pleased with the UK Law Commission's July 2022 report which stated that there is now a 'consensus' on the need for reform of English law on corporate criminal liability, but less pleased that the government has still not decided which, if any, of the Commission's various options for reform to adopt.

The FCA has had a busy year, announcing a number of significant enforcements concerning market misconduct and financial crime, including decisions concerning firms' failure to prevent bribery and corruption. Meanwhile, the SFO has very publicly been criticised for multiple disclosure failings which led to high-profile acquittals of individuals in large fraud and corruption cases. It was not all bad news for the SFO though, with its largest fine levied against a mining and commodities company for bribery. A new head of the SFO will be appointed in 2023.

The cost-of-living crisis, stretched compliance resources, and stressed supply chains are an ideal breeding ground for misconduct. Companies should double down on fostering a culture of compliance, and not turn a blind eye to the increasing use by employees of unauthorised encrypted messaging platforms for doing business.

Investigations – Important trends or developments

A mixed year for the SFO

Disclosure by the SFO should be an area of focus for any defendant in an ongoing investigation. The SFO has, in two independent reviews, been the subject of repeated criticism for disclosure failings which led to the acquittal of individuals in two prominent cases. The Brian Altman KC report made a series of recommendations to improve the way in which the SFO conducts disclosure following the acquittal of individuals allegedly linked to frauds committed by two UK companies (the companies had both entered into DPAs). Another independent report, by Sir David Calvert Smith, this time concerning disclosure in cases against individuals linked to the Unaoil corruption scandal, found multiple failings including inappropriate interaction between the Director of the SFO and a third party.

The SFO will take some solace from its fine of GDP280m against a major commodities trader and mining company, which had pleaded guilty to overseas bribery. The case is the first-ever use of the s1 offence of active bribery under the Bribery Act 2010 (in addition to a s7 charge) against a company. Previous convictions and DPAs under the Act have relied purely on the s7 'failure to prevent bribery' corporate offence.

Other good news in 2022 for the SFO was:

The Economic Crime Bill is expected to extend the SFO's pre-investigation powers to all types of crime. Currently it can only exercise these powers in cases involving fraud and overseas corruption.

The Law Commission concluding that there is a consensus on the need to reform corporate criminal liability – see further below.

No publicity until after charge

A person under a criminal investigation has a reasonable expectation of privacy before they are charged, including when the allegations relate to corruption, bribery and fraud by a company in a foreign country, ruled the Supreme Court in 2022 in Bloomberg v ZXC. The court dismissed an appeal by a financial news service over its reporting of an investigation by an unnamed UK law enforcement body. The chief executive of a regional division of the company had sued the news service for misuse of private information after it reported details of a letter of request sent to a foreign government seeking mutual legal assistance in relation to the investigation. The ruling means that negative publicity associated with a criminal matter involving a business and/or individual should not be reported in the press until after an individual (or the company) is charged.

A focus on AML and kleptocracy

A new Kleptocracy cell has been formed within the UK's National Crime Agency to focus on money laundering, corruption and sanctions evasions targeting corrupt Russian assets. Also, under the Economic Crime Bill, the NCA has been given power to issue information orders even where no suspicious activity report (**SAR**) has been submitted (currently this can only be done after a bank has submitted an SAR), which is likely to lead to more information orders being issued. Penalties for non-compliance include prosecution and fines.

The number of open FCA investigations concerning financial crime is in decline. However, in terms of enforcement outcomes, financial crime, and AML in particular, comes out on top. Since October 2021, 11 fines have been imposed on firms relating to financial crime systems and controls. This represents around half[2] of all fines imposed on firms by the FCA in that period, compared with only two financial crime-related outcomes in the previous year. To a certain extent, this is the result of a high number of open financial crime investigations in previous years working their way through the enforcement process and reaching a conclusion. Nonetheless, it is clear that financial crime remains a high priority for the FCA and it remains intent on sending this message.

The targets of the FCA's AML enforcement activity have generally been brokers and banks.

Important law reforms impacting corporate criminal liability

Proposal to reform corporate criminal liability

The UK Law Commission concluded in July 2022 that there is a consensus on the need for reform of the English law rules on corporate criminal liability. The Commission proposed a number of options aimed at making it easier to make a company (and in particular large companies) criminally liable. While not going nearly as far as U.S.-style vicarious liability, the preferred options included:

– a new corporate 'failure to prevent fraud' offence – using the same model of liability as the failure to prevent bribery, and failure to prevent facilitation of tax evasion offences that we already have under the Bribery Act 2010 and Criminal Finances Act 2017 respectively

– amending the identification principle so that the conduct of a broader range of individuals (extended to 'senior management' not just the 'directing mind and will') can be attributed to the company, bringing the UK more in line with Canada

– a need for further consideration of new failure to prevent offences for ill treatment/neglect in the care sector, human rights abuses and computer misuse

– new civil options to punish corporate fraud, including an administrative penalty regime for failing to prevent fraud, and new public reporting obligations on fraud prevention procedures

– some amendments to individual officer liability.

This is the first time that the Law Commission has acknowledged a consensus on the need for reform. A government response is awaited. Efforts to include a new 'failure to prevent fraud, false accounting and money laundering' offence in the Economic Crime Bill have so far stalled. Want to know more? – see our blog.

Reforms to tackle dirty money

The financial services and professional services sectors have been the subject of much of the law reform in 2022 on money laundering and proliferation financing. They are also among the prime targets for reforms made to sanctions law, shortly after Russia invaded Ukraine. The Economic Crime (Transparency and Enforcement) Act 2022 toughened up UK financial sanctions laws, introducing strict liability for the civil offence of a breach of financial sanctions (replacing the old test of 'knew' or had 'reasonable cause to suspect'). Now, a person's intent or knowledge surrounding a breach of sanctions is irrelevant to the question of whether the UK sanctions enforcer, OFSI, has the power to impose a civil monetary penalty. Changes made in the Act make it easier for the authorities to obtain Unexplained Wealth Orders and also risk banks indirectly being put under the spotlight for the activities of their customers, due to media coverage of these types of orders.

The Economic Crime Bill, which is currently making its way through Parliament, is also aimed at making the UK a less friendly haven for dirty money and at preventing UK shell companies from being used for dubious purposes. Measures include changes to information sharing within the private sector by allowing banks to notify other banks if they are exiting a relationship for money laundering concerns, or where another bank asks for information for financial crime prevention/detection purposes. In addition, it:

– contains enhanced powers for law enforcement agencies to quickly and easily seize crypto assets

– proposes reforms of Companies House, including enhanced powers to query and request information, new identity verification measures, and enhanced data sharing with law enforcement and other stakeholders

– tightens transparency requirements for limited partnerships.

The Bill also tries to lighten the administrative burden for firms. There are changes made to enable firms to be able to pay away suspected criminal property (**CP**) in two new situations: (i) when exiting a client, provided the payment is not over GBP 1000; and (ii) where there are legitimate funds still in the account which are at least equal to value of the criminal property.

Internal investigations – key developments

Chat

Chat applications are increasingly used in the workplace, allowing workers to easily communicate and collaborate with each other. With much of the workforce now working from home at least part of the time, the enhancements in business efficiency and productivity gained from the tools means that the trend is here to stay. As a result, we are seeing more and more chat data in scope for investigations; merely searching standard document types such as efiles and emails is often no longer sufficient. This poses some novel challenges during an internal (and external) investigation for data preservation, collection, document review and production to the authorities. This area is the subject of ever-growing regulatory scrutiny, including by the UK Financial Conduct Authority (FCA).

Document hygiene and the risk of follow-on litigation

When communicating internally during an internal investigation, companies must be alive to the risk of follow-on litigation, and the resulting disclosure obligations. There are currently a number of investor class actions pending off the back of financial crime-related enforcement action.[3] It is too early to tell whether these types of claims will gain much traction. Companies need to assess the risk of such investor action as it may impact decisions made on self-reporting, privilege and cooperation.

Sectors targeted by law reforms or enforcement action

As mentioned above, the financial services and professional services sectors have been on the receiving end of much of the law reform in 2022 aimed at stemming the flow of dirty money into the UK. It has also been the subject of FCA enforcement action, specifically on AML systems and controls failings, a real area of focus for the FCA. Financial crime penalties continue to be among the highest financial penalties imposed on firms, in the regulated financial services sector, by the FCA. Penalties imposed on firms in financial crime cases, since 1 October 2021, total GBP619.7m[4], including a criminal fine of GBP264m[5]. The NCA is recovering over GBP50m of what a major bank had proactively identified as criminal property in a first of its kind civil recovery action in which the account holders were not named in the court proceedings.

The property sector has been targeted by new requirements for overseas owners of UK property to disclose their beneficial ownership and keep it up to date. Entities which fail to comply will face restrictions on selling, leasing and charging their properties, will not be able to obtain legal title to certain newly acquired property and both the entities and their officers may be subject to criminal sanctions or civil penalties.

A House of Lords Committee targeted the telecoms sector, stating it must do more to tackle phishing emails and smishing texts before they reach victims. It recommended that powers should be swiftly introduced via the Online Safety Bill to make telecoms companies more accountable for fraud facilitated through their services (and a duty to report on tech, telecoms and ISPs of details of fraud reports to law enforcement and regulators). The telecoms sector will also be impacted by the coming into force of the UK/U.S. Data Access Agreement coming into force (see more below).

The digital asset ecosystem remains high on the agenda for law reformers and enforcement authorities. Having already been brought into the fold of AML supervision in January 2020, in 2022 a new ‘travel rule’ was introduced requiring certain information on the originator and beneficiary of non-domestic crypto-asset transfers to ‘travel’ with the transfer. Since August 2022 crypto-asset exchange providers and custodian wallet providers have also been included in reporting obligations under financial sanctions laws. The House of Commons Treasury Committee is conducting an inquiry into the use of the crypto-asset industry for money laundering and sanctions evasion.

Finally, the government has announced it will launch a call for evidence to look at the legislative framework that underpins the senior managers and certification regime (**SMCR**) and the FCA and PRA will review their regulatory frameworks for the SMCR. Both the FCA and the PRA have undertaken reviews of the SMCR in the past. Neither resulted in changes being made to the SMCR, but rather noted how successful the SMCR had been in terms of improving culture and driving up standards of conduct across the financial services industry. Against this backdrop, it is hard to see either regulator being in favour of sweeping changes to the SMCR that significantly dilute its requirements.

Cross-border coordination

Companies should assume that UK authorities are speaking to their overseas counterparts. The Director of the SFO has publicly stated on many occasions the importance attached to international cooperation. Both the SFO and the FCA have secondees from overseas enforcement authorities. Two of the FCA's financial crime enforcement outcomes this year, relating to anti-bribery and corruption systems and controls failings, also involved fines and disgorgement or restitution to the Department of Justice in the U.S. The UK sanctions enforcer, OFSI, entered into a new enhanced partnership with its U.S. counterpart, OFAC, this year.

The UK/U.S. Data Access Agreement came into force on 1 October allowing for reciprocal direct access to communications data in cases of serious crime. From a UK perspective, this means that the FCA or SFO can obtain a UK court order which can be served directly on a 'Covered Provider' in the U.S. A U.S. court can make an order which can be served directly on a UK Covered Provider. A Covered Provider includes social media platforms, messaging services, data hosting, cloud storage – basically any business that provides clients with ability to communicate, process or store data. It is aimed at making it much quicker to access electronic data in investigations of serious crime. There are some data protection issues, and it is likely that we will see some challenges to these types of orders.

Predictions for 2023

– Crime increases when individuals are under financial pressure. The cost-of-living crisis coupled with the combination of remote working, reduced/thinly spread compliance budgets, volatile markets and stressed supply chains increases the risk of financial crimes such as corruption, market abuse, fraud and misleading the market. Money mules are an issue that has been highlighted by the FCA. GCs and Heads of Risk will need to be agile to respond, and ensure that compliance policies and speak-up programmes are refreshed and firmly embedded culturally in their organisations. Training may need to be updated to reflect increased hybrid working.

– We are likely to see a government response to the Law Commission options for reform on corporate criminal liability. Any new 'failure to prevent fraud' offence would require GCs to consider whether existing anti-fraud controls are sufficient. This may dovetail with wider corporate governance reforms, which are billed to include a new reporting duty for directors of large companies on steps taken to detect and protect against material fraud.

– The unauthorised use of unmonitored personal devices and encrypted communication applications is widespread, and poses significant enforcement risk particularly to those in regulated sectors. It also impairs the ability of internal investigators to find facts quickly should an allegation of misconduct arise. GCs and Heads of Risk must ensure that policies are fit for purpose, and actively policed.

– Climate change funding (e.g. carbon offsetting programmes or low carbon development or renewable energy) often involves dealing with governments, and therefore presents a higher corruption risk. We expect to see more companies adding ESG to financial crime risk screens as bribery and corruption risk surfaces in carbon offset schemes. Many are already doing so.

– More companies are likely to have to conduct internal investigations focusing on ESG (environmental, social and governance) issues, for example into treatment of workers in their supply chains. Careful thought will need to be given to how these investigations are structured, bearing in mind the chance of follow-on civil or regulatory action.

– Disputes on privilege issues and access to documents and data held abroad will continue as enforcement authorities seek to explore the limits of their powers. GCs will need to be aware of the current interpretation of the authorities' powers, and also any obstacles in meeting these requests, e.g. around data privacy and location of documents. There are likely to be early challenges to the use of the UK/U.S. Direct Access Agreement, including around privilege and data privacy.

– As ever, careful thought needs to be given on deciding whether to self-report, when there is a choice. GCs need to be well informed of any legal obligations to report or immunity incentives to do so, eg antitrust). If there is a choice, and for the SFO in particular, GCs need to understand the cost/benefit analysis of self-reporting. Typically, up to 50% discount to the financial penalty is given for a self-report and cooperation which leads to a deferred prosecution agreement. Conversely, based on prior cases, a one-third discount may be offered for an early guilty plea.

– In the financial services sector, we expect the FCA to intensify its financial crime focus on new market entrants such as e-money firms and crypto businesses.

– Data collection, retention, monitoring and reporting will become increasingly important. The FCA, in particular, has promised to become a more data-driven regulator and will be relying on better analysis of automated data collection as well as web scraping and social media monitoring to identify harm and intervene more quickly.

Key team members

Calum Burnett
Partner – London
Tel +44 20 3088 3736
calum.burnetti@allenovery.com

Arnondo Chakrabarti
Partner – London
Tel +44 20 3088 4424
arnondo.chakrabarti@allenovery.com

Eve Giles
Partner – London
Tel +44 20 3088 4332
eve.giles@allenovery.com

Sarah Hitchins
Partner – London
Tel +44 20 3088 3948
sarah.hitchins@allenovery.com

Brandon O'Neil
Partner – London
Tel +44 20 3088 4187
brandon.oneil@allenovery.com

Amy Edwards
Senior PSL – London
Tel +44 20 3088 2243
amy.edwards@allenovery.com

"A truly experienced team able to mobilise an expert team at short notice in response to a range of corporate crime and regulation issues."

Legal 500 UK, 2023 – Regulatory Investigations and Corporate Crime

"A&O has a very strong corporate base of clientele and expert lawyers to advise on all aspects of corporate business."

Legal 500 UK, 2023 – Regulatory Investigations and Corporate Crime

"This well resourced team sits at the heart of a powerhouse organisation with a global multi-discipline offering in the premier league of complex litigation."

Legal 500 UK, 2023 – Fraud, White Collar Crime

"It can draw on a wealth of knowledge and experience far beyond the bounds of its own specialisms. Very few firms can offer this."

Legal 500 UK, 2023 – Fraud, White Collar Crime

U.S.

With the implementation of new laws and policies focusing extensively on corporate compliance, companies will have to participate in a more careful consideration of their regulatory obligations. Pivotal to this consideration will be companies' ability to effectively spot issues and address potential compliance failures through internal investigations and effective compliance programming. This enhanced focus on corporate compliance is evidenced by the Biden Administration's commitment to increased enforcement efforts both in civil and criminal enforcement. The U.S. Department of Justice (**DOJ**), the Securities and Exchange Commission (**SEC**), and the Commodity Futures Trading Commission (**CFTC**), among other regulatory agencies, have all shown signs of a more zealous enforcement approach, implementing new policies, expanding corporate disclosure requirements, and allocating more resources to enforcement departments. Crypto-assets, insider trading, sanctions, and recordkeeping are all prominent areas of focus.

Investigations trends/developments

Crypto

Enforcement agencies remain focused on crypto-assets. For example, the SEC is adding 20 positions to its Crypto Assets and Cyber Unit. More generally, with the collapse of FTX Trading Ltd., companies should anticipate an increased level of regulatory and enforcement activity around both the FTX case and digital assets as a whole.

Significant enforcement actions in 2022 showed:

- crypto markets must comply with the securities laws, with the SEC charging BlockFi Lending LLC for failing to register the offers and sales of its retail cryptolending product. This was a first-of-its-kind action against crypto-lending platforms, for violating the registration requirements of the Investment Company Act of 1940;
- regulators' willingness to hold decentralized autonomous organization (**DAO**) participants liable for the actions of DAOs, as seen by the CFTC bringing charges against two individuals and a DAO, in a first-of-its-kind action, for violating the Commodity Exchange Act (**CEA**) by: (i) acting as a futures commission merchant without registration; (ii) failing to implement required know-your-customer and anti-money-laundering procedures; and (iii) unlawfully trading off-exchange leveraged and margined retail commodities; and
- regulators are making a push for more aggressive enforcement against the digital assets market, as seen with the CFTC bringing charges against Tether Holdings Limited, and others, for making untrue or misleading statements and omissions of material fact in connection with the U.S. dollar tether token (USDT) stablecoin. The CFTC brought this case, but it included allegations that resemble a traditional SEC enforcement action involving the marketing of a regulated issuance. In addition, there was the first criminal insider trading case involving digital assets being brought in U.S. v *Chastain* and a criminal case being brought in U.S. v *Wahi*, which charged the defendants with wire fraud conspiracy and wire fraud in connection with an insider trading scheme at a global cryptocurrency exchange platform.

Insider Trading

This year has seen many parallel investigations involving insider trading, with charges filed by the SEC and criminal law enforcement. In July 2022, the SEC charged nine individuals in connection with three separate insider trading schemes and all involved parallel criminal charges filed by the U.S. Attorney's Office. This included charges against Ishan Wahi for obtaining material non-public information in his former role as a product manager at a cryptocurrency exchange platform and tipping off his associates ahead of multiple announcements regarding crypto-asset securities. Meanwhile, the CFTC continues to pursue its own insider trading cases under the misappropriation theory, using the anti-manipulation authority under the CEA.

Sanctions

The U.S. has prioritized enforcement actions to ensure companies comply with sanctions and export controls, particularly those against Russia. During a May 2022 conference, Brian Nelson, the Under Secretary for Terrorism and Financial Intelligence at the U.S. Department of the Treasury stated, "enforcement is one of the tools we use to promote compliance, and this is particularly important in the context of our Russia sanctions program…"

Recordkeeping violations

U.S. regulators, particularly the SEC and CFTC, have placed a stronger focus on ensuring that companies are properly monitoring and retaining employee communications. The SEC voted in October to adopt amendments to the electronic recordkeeping, prompt production of records, and third party recordkeeping service requirements applicable to broker-dealers, and security-based swap dealers (**SBSDs**). The goal of these amendments is to modernize recordkeeping requirements and to ensure the recordkeeping rules are adaptable to new technologies.

One of the key changes was to the requirements for electronic records preservation. The amendments change the former requirement to preserve electronic records exclusively in a non-rewriteable, non-erasable format, by now allowing

preservation through an audit-trail method whereby the electronic records are preserved in a manner that permits the re-creation of an original record. Electronic records must be produced to securities regulators in a reasonably usable electronic format.

Corresponding with these changes in recordkeeping policy, the SEC, along with the CFTC, charged 16 Wall Street firms with widespread recordkeeping failures in 2022 with nearly USD2bn paid in combined penalties.

Acting in coordination with the SEC, the CFTC brought charges against a dozen regulated financial entities for widespread recordkeeping and supervision violations, including the use of unapproved messaging platforms such as WhatsApp and Signal by traders and their supervisors.

Significant law reforms impacting corporate criminal liability

Compliance programs firmly under DOJ spotlight

The DOJ has implemented policies throughout 2022 indicating the reaffirmation and strengthening of certain aspects of the Obama-era policies noted in the Yates memo. The Biden administration has focused on improving corporate compliance programs, as evidenced in the DOJ's September 2022 policy announcement, which we covered here.This announcement:

- makes clear that DOJ will now scrutinize executive compensation schemes to determine whether the schemes incentivize compliance
- shows a renewed focus on employees' use of instant messaging for work purposes and the use of personal devices
- lays out ten criteria the DOJ should consider when deciding whether to impose a monitor.

Additionally, compliance specialists now hold key positions within the DOJ's Criminal Division, with both the Assistant Attorney General of the Criminal Division and the Chief of the Fraud Section being former chief compliance offers. This signals that companies must ensure their compliance programs are up-to-date and most importantly that the corporate culture supports an effective compliance program.

Anti-money laundering: new rules on corporate disclosure

The DOJ and other federal regulators, as well as certain state regulators such as the New York Department of Financial Services, continue their trend of increased AML-related enforcement. Two specific areas of focus are foreign banks with touch points in the U.S., and money service businesses, in particular those transacting in digital assets.

The U.S. is on the cusp of implementing corporate beneficial ownership requirements, as outlined in the Corporate Transparency Act (**Act**). In September, FinCEN released the first of three rules implementing the Act, which requires entities to file reports on beneficial owners of the entity, or individuals who applied to create the entity, or register it to do business in the U.S. This rule comes into effect on January 1, 2024, and gives companies up to a year to file their reports. The second rule, relating to who may access beneficial ownership information, for what reasons and what safeguards will be required, and the third rule, relating to revisions to FinCEN's customers due diligence rule, will be forthcoming.

Environmental, Social and Governance (ESG)

The SEC has made significant efforts on enforcement and rulemaking related to ESG. In March 2022, the SEC proposed rules that would require the disclosure of: (i) the registrant's governance of climate-related risks and relevant risk management processes; (ii) the material impact a climate-related risk identified by the registrant may have on its business and consolidated financial statements; (iii) the effect any climate-related risk has on, or which may affect, the registrant's strategy, business model, and outlook; and (iv) the impact climate-related events and transition activities may have on the line items of a registrant's consolidated financial statements. Registrants would also have to disclose information related to their greenhouse gas emissions. On enforcement, the SEC settled charges with a large asset management firm for policies and procedures failures involving funds marketed as ESG investments.

While it is not clear whether these rules will be adopted in their current form, it is clear that the SEC has shown an increased focus on ESG disclosure. Therefore, whether these rules are adopted, companies should ensure compliance programs relating to ESG are up-to-date and are consistent with the company's representations.

Whistleblowers

The CFTC's whistleblower program continues to yield substantial payments to individuals who provide the agency with new information about potential violations of the CEA or the CFTC's regulations. Last year, the CFTC awarded nearly USD200m to a single whistleblower, the largest whistleblower award ever granted by either the CFTC or SEC.

Internal investigations – key considerations

With regulators increasing efforts related to criminal corporate enforcement, it is important that companies continue to pay close attention to the actions of their employees. Therefore, the company's ethics and compliance programs must be designed and implemented in a way that is unique to the business they were created for. Based on regulators' current focus, companies should expect to:

- have a procedure in place to actively and effectively manage whistleblower concerns and know when an internal investigation into reported suspected misconduct is required
- ensure privilege over the internal investigation is maintained, including being mindful of informing interviewees of their rights under Upjohn, particularly when dealing with cross-border investigations
- be mindful of data privacy and bank secrecy issues when conducting an internal investigation. If regulators become involved, a way to avoid data privacy or bank secrecy issues is to obtain the data through a Mutual Legal Assistance Treaty (MLAT).

Sectors targeted by law reform or enforcement

Antitrust: increased enforcement – focus on algorithmic pricing and potential for AI coordination and criminal monopolisation

At the 21st Annual International Competition Network Conference, the DOJ's Antitrust Division signalled an increased focus on risks in algorithmic pricing and AI coordination. Assistant Attorney General, Jonathan Kanter, suggested that companies should be cognizant of the risk of collusion in price-fixing through technological means and noted that the DOJ was increasing its capacity to pursue investigations and enforcement actions in this area.

Additionally, the DOJ's Antitrust Division has taken a more active approach towards criminal monopolisation and has secured a guilty plea in the first criminal monopolisation case since 1978. In this case, an individual was charged with, and pled guilty to, one count of attempted criminal monopolisation, in violation of Section 2 of the Sherman Act.[12]

Cross-border coordinated investigation or enforcement activity

Corruption considered a U.S. national security threat

Corruption enforcement, particularly related to corporate crime, is regarded as a core aspect of U.S. national security. The White House's December 6, 2021, Strategy on Countering Corruption calls for increased intelligence-sharing between the U.S. and foreign partners, and deepening cooperation through partnering with countries in joint investigations and prosecutions. Companies should expect to see an expansion of laws across all regulatory agencies where gatekeepers of the financial systems, such as lawyers and accountants, are held accountable for potentially complicit misconduct.

Digital Assets: involvement outside the United States

The CFTC continues to pursue activities involving digital asset markets both within and outside of the United States. Last year, the CFTC brought 18 actions involving conduct related to digital assets. This represents more than 20% of all actions filed during the year. Many of these were cross-border actions involving companies and individuals located outside of the United States who were engaged in activities that have a connection to U.S. markets.

12 United States v. Zito, Crim. No. 1:22-cr-00113, at 4 (D. Mont. Sept. 19, 2022).

Predictions for 2023

Looking forward, companies should expect to see a continued prioritization of increased enforcement over corporate behavior, and companies should expect to face greater scrutiny from regulators. As such, companies should continue to advance and monitor their compliance programs to ensure for adequate monitoring, prevention and remediation of corporate misconduct. Future areas of focus include:

Cybersecurity

Proposed cybersecurity amendments will likely see an increased focus on cybersecurity responses. With the increased use of digital technologies, crypto-assets and the permanent shift to a hybrid work environment, the SEC proposed amendments in March to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting.

The proposed rules would require:

– disclosure of material cybersecurity incidents in the Form 8-K reporting within four days of an incident

– updates to any previously reported incidents

– disclosure of cybersecurity risk management and strategy

– disclosure of cybersecurity governance, including the board's oversight of cybersecurity risk

– disclosure regarding the board's cybersecurity expertise.

The amendments also propose to amend the foreign disclosures to align more with the domestic disclosures.

While these proposed amendments have not been finalized, we predict that they indicate an increased focus and importance put on cybersecurity.

Crypto

Market participants should expect to face greater scrutiny from regulators in the crypto space. This year, regulatory agencies have brought many enforcement actions against cryptocurrency and asset companies for the unregistered sale or offering of securities. One such case, Ripple Labs, is still being litigated. According to Ripple CEO Brad Garlinghouse, if Ripple loses, most tokens trading on platforms in the U.S. would be deemed securities, meaning those platforms would have to register with the SEC as broker dealers. Therefore, looking towards the future, market participants should understand how securities laws may apply to digital asset borrowing and lending activities, even in cases where the digital assets themselves may not be securities.

Compliance

Companies should expect to see more onus put on their CCOs to ensure effective compliance, with Kenneth Polite, Assistant Attorney General, DOJ's Criminal Division, considering whether 'requiring both the CEO and the CCO to certify at the end of the term of the agreement that the company's compliance program is reasonably designed and implemented to detect and prevent violations of the law, nd is functioning effectively…'

Life Sciences

Pharmaceutical companies should expect focus to remain on drug pricing and access to generics. The Food and Drug Administration is expected to continue its scrutiny of vaping products, particularly with more states implementing legislation for the sale of recreational cannabis and the growing popularity of cannabis-derived products, such as CBD.

Key team members

Eugene Ingoglia
Partner – New York
Tel +1 212 610 6369
eugene.ingoglia@allenovery.com

Jonathan Lopez
Partner – Washington, D.C
Tel +1 202 683 3888
jonathan.lopez@allenovery.com

Claire Rajan
Partner – Washington D.C.
Tel +1 202 683 3869
claire.rajan@allenovery.com

Jonathan Flynn
Senior Counsel – Boston
Tel +1 202 683 3858
jonathan.flynn@allenovery.com

Brigitte Sykes
Associate – New York
Tel +1 212 610 6385
brigitte.sykes@allenovery.com

Elena Aguirre
Law Clerk – New York
Tel +1 212 610 6497
elena.aguirre@allenovery.com

"The firm has a dynamic white-collar group that does high-profile work."
Chambers USA, 2022 – New York

"Allen & Overy does a tremendous job in advising us on complex and nuanced regulatory questions that have no precedent."
Chambers USA, 2022 – D.C.

"They're highly qualified and clearly able to handle very complex and detailed cases. They are very experienced and have displayed a high level of in-depth understanding."
Chambers USA, 2022 – D.C.

"The team provides advice at the highest level possible, is very quick to respond and combines law and compassion, which is a rare trait in the legal industry, but in the white-collar practice, when representing individuals in extremely difficult situations, is a very important trait."
Legal 500, 2022

"Intelligence, professionalism, deep understanding of enforcement mechanisms, compassion. The team is genuinely caring and involved in the client's situation."
Legal 500, 2022

For more information, please contact:

London

Allen & Overy LLP
One Bishops Square
London
E1 6AD
United Kingdom

Tel +44 20 3088 0000
Fax +44 20 3088 0088

Office contact

Amy Edwards
Senior PSL – London
Tel +44 20 3088 2243
amy.edwards@allenovery.com

Global presence

Allen & Overy is an international legal practice with approximately 5,600 people, including some 580 partners, working in more than 40 offices worldwide. A current list of Allen & Overy offices is available at www.allenovery.com/global_coverage.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen & Overy (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen & Overy LLP and Allen & Overy (Holdings) Limited are authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term partner is used to refer to a member of Allen & Overy LLP or a director of Allen & Overy (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of the members of Allen & Overy LLP and of the non-members who are designated as partners, and a list of the directors of Allen & Overy (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.

GB
CS2212_CDD-71426_ADD-104973