ALLEN & OVERY

Cross-Border White Collar Crime and Investigations Review

2022

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.

More countries are introducing or amending financial crime laws, new types of businesses are being brought into the scope of existing laws, and there are increased expectations on corporate behaviour from a wider range of stakeholders. In-house counsel need to be nimble footed to help organisations adapt to new expectations, and mitigate the impact of issues that arise.

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 2022.

Looking ahead – managing key challenges in 2022

We asked our global white collar crime team for their views on key challenges in 2022 for in house investigations teams and white collar crime lawyers, and how to manage the associated risks.

Understand evolving expectations on corporate accountability

Expect increased scrutiny of corporate behaviour – Higher standards and expectations on corporate accountability have manifested in different ways across the globe. However, 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 some countries (France, Germany, Belgium) there are new corporate vigilance obligations either in force or proposed. In addition, pressure is being exerted by a broader range of stakeholders. Activist shareholders, employees and others are using both litigation and reputational levers to hold companies to account for environmental harms and human rights violations.

How you should respond – Prevention is better than cure so companies should check that compliance and whistleblowing procedures are working as intended. 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.

Don't take your eye off intermediaries

The use of intermediaries remains a high corruption risk – Like many previous years, the enforcement authorities took action in 2021 on corrupt payments made to third parties including those concealed as, for example, consultancy fees, sponsorship or charitable donations. Post-pandemic pressure on supply chains means that some companies may be keen to enter business arrangements with new partners, quickly.

How you should respond – Companies must ensure that their policies and procedures around the use of such business partners are properly implemented, and reviewed on a regular basis to reflect the business as it evolves. Ensure that commercial pressures are not trumping adequate due diligence.

Old and new financial gatekeepers must keep up to date with AML compliance

Expect tougher anti-money laundering and counter-terrorist financing laws – Every jurisdiction surveyed this year is bolstering anti-money laundering and counter-terrorist financing laws, many following the recommendations from the Financial Action Task Force. The traditional financial gatekeepers such as banks are prime targets for enhanced regulation and tougher laws. But a broader range of gatekeepers are increasingly being bought into the frame with regulations being expanded to catch virtual asset service providers and fintechs. Whilst automation and AI can do some of the heavy lifting on AML compliance, enforcement shows that performance of AI will only be as good as (1) the data it relies on, and (2) the quality of the human decision making at the point when the system raises a red flag. We expect to see continued close scrutiny and rigorous enforcement in this area, particularly around weak systems and controls.

How you should respond – All types of business, not just those in finance, should identify money laundering risks and implement controls, with appropriate senior management oversight, to mitigate them. Compliance functions must be adequately resourced. Staff should be sufficiently experienced and feel empowered to independently question decisions taken by others.

Consider the risk of corporate criminal exposure

Expect law reform on corporate criminal liability – Proposed and actual legislative reform in several jurisdictions is aimed at making it easier to convict large companies of a criminal offence. Some jurisdictions have adopted, or are considering adopting (e.g. Australia), the UK Bribery Act 2010 s7 model of 'failure to prevent' bribery. There is pressure on the UK government for this type of offence to apply to a broader category of financial crimes.

How you should respond – Any analysis of corporate exposure following allegations of misconduct should factor in the jurisdictions involved, and the risk of corporate (and individual) liability. Companies should reduce their financial crime risk, and maximise their chance of successfully mounting an 'adequate procedures' defence, where applicable, by implementing an effective compliance programme. Companies which formulated their policies some years ago should review relevant guidance, update policies, provide regular training to staff and ensure that both senior and middle management set the right tone in their behaviour and communications. This is particularly so given the move to more remote working. 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 enough to inform the design, implementation and effectiveness of compliance programmes.

Ensure corporate culture supports effective compliance

Expect more scrutiny of how corporate culture and compliance interact – Recent bribery enforcement suggests that just 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 'failure to prevent' type offences. How the policies and procedures are embedded in an organisation is critical to making them effective. Large global companies with sophisticated ABAC policies and procedures have fallen foul of bribery laws where the culture at the company has permitted bribery to take place. We expect to see continued scrutiny by authorities on 'tone from the top' and the tone from within (i.e. middle management).

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 remediation not only limits damage for the company but may be viewed positively by the authorities.

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 means that businesses can increasingly end up as pawns, often being stuck between conflicting requirements that require delicate navigation.

New data and national security laws in China need to be carefully considered during any investigation which has a Chinese nexus. The U.S. government has explicitly said that fighting corruption is now a U.S. national security priority – meaning more FCPA enforcement. There are new sanctions aimed at overseas corruption and human rights abuses (e.g in the US, EU and UK). And counter-measures/blocking rules (eg. in China and the EU) are aimed at limiting the impact of some sanctions.

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.

Don't underestimate the expanding global enforcement web

Expect greater international collaboration and information sharing among enforcement agencies – Despite the geopolitics, there is undoubtedly more collaboration between some jurisdictions either informally or formally. A June 2021 White House memo states that working with international partners on anti-bribery enforcement is a priority. The new European Prosecutors Office started work in 2021 and is already involved in investigations. More countries are entering into bilateral cooperation agreements in the fight against financial crime.

How you should respond – Any investigation that has touch points in more than one jurisdiction will likely involve the authorities talking behind the scenes at the investigation, charging and settlement stages. This should impact a company's strategic decisions, particularly around interactions with authorities during an investigation.

Looking after your data

Expect more attention from regulators and enforcement agencies as they double down on data protection and cybersecurity failures – More jurisdictions are introducing data protection laws or national security laws which apply to a company which needs to move or use data during an internal or external investigation (e.g. Hong Kong SAR, Mainland China, South Africa).

How you should respond – Understand the legal and enforcement context that applies to any use or movement of company records, documents or any other data during an investigation. There is no substitute here for being attuned to the attitudes of the authorities involved, and knowing the options when navigating a path which deals with data privacy and other legal concerns whilst at the same time enabling a company to investigate allegations of misconduct or meet requests from foreign regulators.

Expect enforcement agencies to want to see evidence stored abroad – Criminal authorities are keen to have the ability to access data held abroad relating to a company under investigation. There have been law reforms or proposed law reforms in the US, UK, EU, South Africa and Australia all aimed at making it easier for authorities there to obtain data directly from foreign third party communication service providers. There have been legal challenges (for example in the UK, Australia, Belgium) over authorities' ability to access data or compel production of documents abroad.

How you should respond – Lawyers involved with external investigations need to understand the proper remit of authorities' powers to order or seek disclosure of data held abroad (e.g. by a holding company or by a third party communications service provider). This insight should inform a workable, risk-reducing approach to disclosure as well as capitalise on cooperation credit if a company decides to provide documents that go beyond what an authority is legally entitled to compel.

Expect cybersecurity to remain a priority – Companies face hefty fines, and cybersecurity remains a favourite on many authorities' compliance and enforcement agendas. U.S. SEC Chairman Gary Gensler has prioritised cybersecurity, including cyber-hygiene and incident reporting. In Australia, ASIC has brought its first court action against a company for failing to have adequate cybersecurity systems in place. The pandemic provided a breeding ground for cyber criminals to infiltrate organisations on a scale not seen before, with ransomware the malware of choice for many seeking to cause maximum disruption to businesses during already challenging times.

How you should respond – The most effective way to address the threat of these attacks is to invest in strong defences and experienced personnel whilst implementing robust processes and procedures so that a business stands ready to react, respond and remediate any incidents that occur. Read more on our cybersecurity series: "Infiltrate, extort, repeat".

Understand the risk/benefit analysis on 'cooperation'

Expect to have to weigh up the pros and cons of cooperation – Many developed regimes encourage a company under investigation to cooperate with the authorities in order to obtain 'credit' which can, in turn, mean a greater chance of avoiding a corporate conviction and help to secure a discounted fine.

How you should respond – Corporate appetite for cooperation will depend on the perceived benefits. Consider whether penalty discounts are sufficiently differentiated from a company that is convicted following a guilty plea or does not initially self-report. The degree of cooperation that a company will want to engage in should be informed by an understanding of the advantages and disadvantages, its approach in other jurisdictions, and also an analysis of the risk of corporate criminal liability, which varies by jurisdiction and, as above, is another evolving area of law.

Be alive to the pinch points on privilege

Expect more pushback when claiming legal privilege – This has been a challenge for some years. There is often a tension between an authority's expectations of cooperation, and rules on legal professional privilege. Some authorities are hardening their stance on privilege, eg by demanding either third-party certification of privilege claims or exercising or demanding more power to determine the applicability of legal privilege in particular cases.

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.

Our lawyers have a vast amount of 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

2021 saw another year of high levels of regulatory activity in Australia. The regulatory landscape has continued to experience significant shifts against the backdrop of the COVID-19 pandemic's impact on Australia's economic and political spheres. ASIC, the financial services regulator, has departed from its much-publicised and controversial "why not litigate" approach in favour of an approach that prioritises promoting Australia's economic recovery. Parliament has enacted legislation in a wide range of areas impacting on white collar crime and investigations, with more reform on the horizon, including in relation to money laundering and terrorism financing, foreign bribery, and corruption. However, legislative priorities may shift in the lead-up to, and aftermath of, Australia's next federal election, which must be held by May 2022. The first enforcement action against a company for cybersecurity failings is almost certainly a sign of more to come.

Belgium

In 2021, criminal enforcement in Belgium was robust, focussing on various crimes, such as complex fraud and money laundering involving financial intermediaries, corruption, cybercrime, and environmental pollution. The Belgian legislator continues to develop a Business and Human Rights framework that will serve as an additional tool to sanction breaches of fundamental rights. Private companies are increasingly sensitive to criminal law risks, including in the field of M&A, where compliance in the broad sense of the word has become a focal point. Looking forward to 2022, we expect these trends to continue and intensify. The implementation of the EU Whistleblowing Directive will result in increased disclosures, fuelling new investigations and criminal prosecution. Finally, also under EU influence, the operationalisation of the European Public Prosecutors Office will elevate financial crime on the enforcement agenda, strengthen cross-border enforcement, and favour contentious litigation over out-of-court settlements.

Mainland China

New data protection and data security laws in China add considerably to the complexity of conducting cross-border investigations with a nexus to China, and meeting information requests from foreign regulators. A new 'anti-sanctions' regime is aimed at counteracting foreign sanctions and trade controls, and multinational companies doing business in China are expected to follow. The ABAC regime continues to develop with a greater focus on enforcement against private company offerors of bribes. The real estate and construction industry has been the primary focus of criminal actions in 2021, and the life sciences industry remains the primary focus of administrative penalties. Looking ahead to 2022 we can expect to see more enforcement actions in these areas.

France

France remains a hub for white collar crime enforcement. Spearheaded by the National Financial Prosecutor's Office (**PNF**), the white collar criminal enforcement landscape continues to move towards greater collaboration with overseas enforcement authorities, corporate settlements, and heavy fines. The fight against money laundering, tax evasion and corrupt practices remains at the forefront of enforcement action, alongside a rising number of investigations in the area of Environmental and Social Governance (**ESG**). Several bills have been presented by MPs to the French Parliament over recent months, relating in particular to the fight against corrupt practices, the internal investigation process and the protection of whistleblowers. Depending on how they progress through the French Parliament, they may give rise to new obligations for corporates with a French nexus in 2022.

Germany

2021 yielded many developments in the field of white collar crime enforcement and investigations in Germany. In July, the German Federal Court of Justice (*Bundesgerichtshof*) ruled that obtaining a refund of unlevied withholding tax in connection with a cum/ex trade constitutes the criminal offence of tax evasion. Against this backdrop, criminal enforcement against participants in these trades continued unabated, with several dawn-raids being conducted and new bills of indictment being issued. Criminal proceedings into cum/ex trading are now directed against more than 1000 suspects, including C-level executives of international banks.

In addition, the German legislator enacted a Supply Chain Due Diligence Act, which will come into force on 1 January 2023. The German lawmaker also expanded the scope of the criminal offence of money laundering with effect from 18 March 2021. The Corporate Sanctions Act, which was supposed to introduce more severe corporate fines and new rules for conducting internal investigations, was not passed. The previous German federal government also failed to enact the Whistleblower Protection Act, even though EU member states were obliged to transpose the underlying EU directive into national law by 17 December 2021. The new German federal government has announced that it will readopt these unfinished legal initiatives.

Hong Kong SAR, China

Personal data laws were amended in Hong Kong in 2021, meaning that businesses will need to be particularly careful about the expanded investigation and enforcement powers of the Privacy Commissioner for Personal Data (**Privacy Commissioner**). Despite Covid-19, financial regulatory enforcement actions have regained momentum. The Securities and Futures Commission (**SFC**) continues to focus on "high-impact" cases against financial institutions, listed companies and senior executives, with a targeted approach to enforcement. The Hong Kong Exchanges and Clearing Limited's (**HKEX**) enforcement agenda and power, as along with the Financial Reporting Council's (**FRC**) enforcement actions, have become more advanced and proactive. Various local regulators have increased their level of collaboration to combat corporate fraud, misconduct, and malpractices in the financial market.

Netherlands

The Covid-19 pandemic has resulted in fewer criminal enforcements in the Netherlands. Nevertheless, corruption and other types of economic and financial crime remain high priorities for the Dutch enforcement authorities. The Dutch regulators and the Dutch Public Prosecution Service (the **DPPS**) continue to pay close attention to supervised gatekeepers of the financial system for non-compliance with Anti-Money Laundering (**AML**) regulations and sanctions law. In cases where a legal entity enters into a settlement with the DPPS, there seems to be an increased focus on the prosecution of individuals. In the criminal tax field, in 2022 we expect more attention to be given to matters where the integrity of the financial sector is under scrutiny, such as dividend stripping. Cybercrime is high on the enforcement agenda. We also expect more cases that will relate to business responsibility for human rights. A follow-up to the legislative processes surrounding a draft bill related to judicial review of high-value settlements with the DPPS is expected.

South Africa

South Africa's white collar crime framework continues to develop in the wake of a series of "state capture" enquiries by the Special Investigating Unit (**SIU**) and National Prosecuting Authority (**NPA**). Together with former President Zuma's longstanding corruption trial relating to arms procurement in the late 1990s and activism on corporate accountability and environmental issues, this has led to clarifications regarding key issues in the investigation and prosecution of white collar crime. While South African courts have been particularly active in the past year, Parliament, National Treasury and regulators such as the South African Revenue Service (**SARS**) and Financial Intelligence Centre (**FIC**) have taken steps to consolidate and amend South Africa's regulatory framework to enhance corporate transparency and improve personal data and crypto asset regulation – developments likely to unfold in the next year. Major cross-border investigations to watch include the cum/ex banking scandal while poaching continues to be a key focus of cross-border law-enforcement.

United Arab Emirates

2021 has seen the UAE implement a raft of measures to enhance its AML and CTF capabilities, including making key amendments to AML legislation, the issuance of new joint agency guidance on AML and CTF compliance and the establishment of a new federal AML/CTF agency and a money laundering specialist court in Dubai. These actions have implications for both the UAE's onshore jurisdiction and its key offshore jurisdictions including the Dubai International Financial Centre (the **DIFC**) and the Abu Dhabi Global Market (the **ADGM**).

These developments place a key focus on expanding the scope of the UAE's AML/CTF regime and increasing the monitoring of high-risk sectors for financial crime (including emerging areas of the financial services industry such as virtual assets).

Enhancing coordination and cooperation both across jurisdictions and between agencies has also been a priority.

There have also been developments which have aimed to enhance the UAE's anti-bribery and corruption compliance credentials, make whistleblowing protections clearer and make corruption and compliance reporting easier.

The pace of regulatory change and development (in particular in the area of combatting financial crime) is likely to continue and so it remains of crucial importance for businesses to have robust systems and controls in place to understand, adapt to and ensure ongoing compliance with the quickly changing and increasingly complex regulatory environment in the UAE.

United Kingdom

Money laundering was firmly in the sights of the UK authorities in 2021 and will remain so in 2022. The FCA managed to secure a guilty plea and a large fine from a bank in its first prosecution of a bank under the UK Money Laundering Regulations and the UK's entire CTF/AML regime is currently under review. The AML supervision of crypto assets will likely evolve in 2022 as it is considered a high risk area.

New criminal offences relating to defined benefit pension schemes were introduced, but the consultation on corporate criminal liability more generally is still ongoing, with a report expected from the Law Commission in early in 2022. Big Tech companies are under pressure to reduce online harms, with new criminal offences possibly being introduced in 2022 via the Online Safety Bill.

The Serious Fraud Office is likely to be focussing on frauds on the public purse committed during the pandemic. It will also be trying to regain its enforcement momentum after some difficult (for the SFO) court decisions which curtailed its ability to obtain documents held abroad and criticised the SFO's lack of disclosure in some high profile cases. 2021 saw the number of new SFO corporate criminal investigations fall to the lowest number (four) in over a decade.

Investigations into ESG related issues are becoming much more common, as investors and employees seek to exert pressure on companies to improve treatment of workers in supply chains and reduce environmental impact.

United States

The Biden Administration, including the President himself, has signalled an intent aggressively to ratchet up enforcement efforts on many fronts, spanning both the criminal and civil contexts. The U.S. Department of Justice (DOJ), Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), and Federal Trade Commission (FTC), among other regulatory agencies, have all shown signs of a more zealous enforcement approach, which marks a sea change in the regulatory landscape compared to that of the prior administration. The shift toward an aggressive regulatory environment includes the deployment of more proactive investigative methods, a greater focus on prior misconduct, increasingly stringent corporate resolutions, and broader theories of corporate liability. These changes have undeniable implications for companies in all sectors, such as: (1) the need for robust compliance programs that incorporate strong prophylactic controls and remediate misconduct appropriately; and (2) the increasing importance of expert legal advice in navigating the heightened expectations of regulators and understanding the regulatory risks companies face in conducting their operations.

Australia

2021 saw another year of high levels of regulatory activity in Australia. The regulatory landscape has continued to experience significant shifts against the backdrop of the COVID-19 pandemic's impact on Australia's economic and political spheres. ASIC, the financial services regulator, has departed from its much-publicised and controversial "why not litigate" approach in favour of an approach that prioritises promoting Australia's economic recovery. Parliament has enacted legislation in a wide range of areas impacting on white collar crime and investigations, with more reform on the horizon, including in relation to money laundering and terrorism financing, foreign bribery, and corruption. However, legislative priorities may shift in the lead-up to, and aftermath of, Australia's next federal election, which must be held by May 2022. The first enforcement action against a company for cybersecurity failings is almost certainly a sign of more to come.

Investigations trends/developments

A revised enforcement approach to support economic recovery

The Australian Securities and Investments Commission (**ASIC**) has been active, with 159 investigations and 26 civil penalty proceedings in the year to June 2021.

ASIC indicated in March 2021 that it would be moving away from its "why not litigate" approach, which it adopted in 2018 during the Royal Commission into Misconduct in the Banking, Superannuation and Financial Securities Industry (**Royal Commission**). Instead, ASIC announced that it would adopt a "lighter and more impactful" approach, including by holding "express investigations" that featured a high level of cooperation with businesses. This change was spurred by criticisms from the Australian Government and Reserve Bank of Australia that ASIC was not showing the commerciality required in the current economic climate, and that its aggressive stance could deter the lending necessary to assist Australia's post-pandemic economic recovery.

Shortly after ASIC committed to this new approach, it also announced changes in its top personnel, including that Joe Longo would become its new chair. That announcement — and Mr Longo's first media interview — emphasised ASIC's new priority of supporting Australia's economy and businesses.

A focus on cybersecurity

ASIC's Corporate Plan 2021-2025 includes a focus on cybersecurity. ASIC is bringing its first court action against a company for failing to have adequate cybersecurity systems in place, which is proceeding to trial in April 2022. The proceedings relate to a business that provides financial advice and its authorised representatives. One of the authorised representatives of the business was subject to a 'brute force' attack whereby a malicious user successfully gained remote access to its server. The attacker spent more than 155 hours within the server, which contained sensitive client information.

ASIC alleges that the business failed to implement (including on the part of its authorised representatives) adequate policies, systems and resources which were reasonably appropriate to manage the cybersecurity risk.

ASIC has asked for a penalty in an amount thought appropriate by the Court. The civil penalty provisions have recently been amended such that the maximum penalty is now the greater of: (1) AUD10.5 million; (2) three times the benefit derived from (or detriment avoided by) the contravention; or (3) 10% of revenue up to AUD525 million.

More enforcement activity is expected in this area.

More encouragement for whistleblowers

ASIC continues to encourage whistleblowing individuals. It urged businesses in October 2021 to ensure that their whistleblower policies were compliant with regulatory requirements and working as intended, and released a new immunity policy, offering immunity from civil and criminal liability, to the first reporting individual, for contraventions of the Corporations Act 2001 (Cth) relating to market misconduct such as insider trading and market manipulation. Ongoing and significant cooperation by the first reporting individual is required by ASIC/the Commonwealth Director of Public Prosecutions (**CDPP**) in order to maintain the safe harbour of the policy.

While it is in many respects similar to the Australian Competition and Consumer Commission's (**ACCC**) immunity policy, one of its notable differences is that it only applies to individuals and not corporations.

While we are yet to see the policy employed, we do expect that it will contribute to an increase in investigation and prosecution activity for market misconduct offences.

Significant law reforms impacting corporate criminal liability

"Phase 1.5" of Australia's anti-money laundering and counter-terrorism financing (**AML/CTF**) reforms came into effect in June 2021, with a view to making it easier for reporting entities (being entities that provide designated services under the AML/CTF Act of 2006, such as financial, gambling, bullion or digital currency exchange services) to comply with their reporting obligations. We summarised the key changes in these reforms in our article here.

Further reforms are on the horizon, with Australia's Legal and Constitutional Affairs References Committee currently conducting an inquiry into the adequacy and efficiency of Australia's AML/CTF regime (due to report by March 2022), and additional impetus provided by the recent release of the Pandora Papers and law reforms proposed in the United States such as the ENABLERS Act. The Committee is likely to consider extending the AML/CTF reporting regime to professions such as lawyers, accountants and real estate agents.

"Failure to prevent" offence inches forwards but still not in force

Australia's efforts to amend foreign bribery laws and introduce a federal anti-corruption watchdog have languished for several years. However, in 2021 the Government recommended that the Senate approve proposed foreign bribery law amendments. The Foreign Bribery Bill, which is likely to be passed in the coming months, proposes a new criminal offence of bribery by an associate (for which a corporation may be convicted unless it has in place "adequate procedures" designed to prevent that conduct) that is punishable by a fine that is the greater of:

– AUD21million;

– three times the value of the benefit provided; or

– 10% of the corporation's annual turnover.

This offence is very similar to the 'failure to prevent bribery' offence in the UK Bribery Act 2010. We summarised other key elements of this Bill in our article here. The Bill also allows for deferred prosecution agreements.

While the Australian Government announced in 2018 that it would establish a Commonwealth Integrity Commission to investigate corruption by Commonwealth employees, a consultation draft of legislation that would provide for this was only released in November 2020, and has not yet been introduced into the Australian Parliament. However, public debate about the proposed Commonwealth Integrity Commission — and its associated delays — has intensified in recent months, with high-profile investigations being conducted by the New South Wales and Victorian anti-corruption bodies.

First modern slavery reports

The first modern slavery statements mandated by the Modern Slavery Act 2018 (Cth) were due in March 2021. The Act requires entities with annual consolidated revenue of more than AUS$100 million to report on the risks of modern slavery in their operations and supply chains.All modern slavery statements are published on a public register administered by the Australian Border Force.

The Act does not impose any penalties for non-compliance, but the framework is set up to maximise transparency and ensure entities are publicly accountable to address modern slavery risks. The Act is due for its first review, commencing in January 2022. This review is likely to include consideration of whether the reporting threshold should be reduced to AUS$50 million. The equivalent New South Wales legislation, the Modern Slavery Act 2018 (NSW), had included more stringent reporting requirements and stronger enforcement mechanisms. However, the Modern Slavery Amendment Bill 2021 (NSW) makes a number of important changes to it, including removing the imposition of penalties for failing to prepare a modern slavery statement. It is expected to come into force in January 2022.

Australia's first debarment regime

Australia does not currently have a nationally coordinated debarment regime. However, the state of Western Australia (**WA**) has introduced a debarment regime that came into effect on 1 January 2022. The regime is retroactive so it may affect contracts in place before that date.

Under the WA regime, the decision to debar a supplier is discretionary and made in the public interest. Debarred suppliers will be precluded from being awarded contracts (or extensions of existing contracts) for the supply of goods, services or works to a WA state agency. For breaches of certain serious criminal offences (eg fraud, bribery, money laundering), debarment can be ordered for a maximum of five years. For breaches of legislation considered less serious (eg in tax law), the maximum debarment is two years.

Importantly, debarment under the Western Australian regime can extend to conduct committed in foreign jurisdictions. The regime includes a provision that allows the decision-maker to exclude suppliers based on conduct in other jurisdictions provided the conduct is "of a kind" described in the regulations.

This is in combination with an "affiliate" debarment power that allows the state of Western Australia to preclude Australian subsidiaries of international corporations that have been found to have been engaged in debarment conduct in another jurisdiction from consideration for public contracts in Western Australia.

Internal investigations – key developments

ASIC has shown a greater willingness to challenge companies' lack of cooperation and claims of legal professional privilege over documents that they have been compelled to produce.

This has resulted in courts upholding production notices issued by ASIC over large numbers of documents not only in a company's physical possession, but also in its custody or under its de facto control in other locations. In *Maxi EFX Global AU Pty Ltd* v *ASIC* [2021] (FCAFC 59) the Court found that Maxi was required to produce documents to ASIC that were held by third party service providers in Belize, Cyprus and Israel.

In line with its "lighter and more impactful" approach, ASIC has urged companies to recognise and acknowledge wrongdoing early so that its investigations can be brought to a close effectively and efficiently. In practice, this may mean that companies should consider engaging with regulators at an earlier juncture.

ASIC has also had notable successes in challenging privilege claims, including in *ASIC v RI Advice Group Pty Ltd* [2020] FCA 1277 in respect of a document which had been already disclosed to a third party. The Court found that the document was not privileged because there was no direct evidence that its dominant purpose was to provide legal advice. This allowed for the inference that there were multiple purposes to the document. In any event, if the document had been privileged, the privilege had been waived as it had already been provided to a third party without any stipulations on privilege being retained.

The decision highlights the importance of retaining contemporaneous evidence of the purpose for the creation of a document, and taking great care not to waive privilege if providing it to a third party, including an investigating authority.

Sectors targeted by law reforms or enforcement action

The financial sector continues to be a focus for enforcement action, with insurance, superannuation, stock market, auditor, and credit misconduct representing key enforcement priorities for ASIC. This year ASIC commenced proceedings against a "big four" Australian bank for insider trading, unconscionable conduct, and breaches of its Australian financial services licensee obligations, which is only the third insider trading case brought against a company in Australia.

The gaming sector continues to receive significant regulatory scrutiny. This includes investigations being launched by the Australian Transaction Reports and Analysis Centre into the compliance of three of Australia's largest gaming operators with the AML/CTF regime following numerous state-based inquiries and Royal Commissions.

The ACCC is likely to continue to prioritise cases concerning cartel conduct and anti-competitive conduct, without targeting any particular sectors, and refer serious cases to the CDPP. This is notwithstanding the fact that its record of referring cases to the CDPP has been mixed:

– The CDPP's prosecution of a global shipping company (which pleaded guilty) for criminal cartel conduct led to a conviction in February 2021, and a fine of AUD24 million.

– The CDPP was unsuccessful in prosecuting a healthcare company in Australia's first criminal cartel case (for bid rigging and price fixing) to proceed to trial by jury, with the company, its chief executive officer and former employees being acquitted by the jury in June 2021.

– The CDPP withdrew criminal cartel charges against the Construction, Forestry, Maritime, Mining and Energy Union due to challenges posed by the extended passage of time since the alleged conduct occurred. This case was one of the first times that competition laws were applied to industrial relations negotiations, and it is expected this will have precedential value.

– The CDPP's first criminal cartel case in respect of the financial services industry continues to face challenges, with the CDPP being ordered in November 2021 to revise its indictment for the third time, and withdrawing charges against several defendants. The case is set down for a trial by jury in 2022.

We expect to see further ACCC enforcement action.

Cross-border coordinated enforcement activity

We regularly assist companies based outside Australia in responding to production requests from Australian regulators investigating corporate contraventions and AML/CTF breaches, including in the cryptocurrency sector. A new law (the Telecommunications Legislation Amendment (International Production Orders) Act 2021) aimed at allowing investigating agencies to access data directly from foreign communications service providers will add to cross-border information flows. The law is an early part of a network of bilateral agreements, starting with the U.S. CLOUD Act, and the UK Crime (Overseas Production Orders) Act 2019, aimed at easing access by investigating authorities to communications data overseas.

We have also seen ASIC coordinating investigations with foreign agencies, including the Federal Bureau of Investigation in relation to an investigation into a cryptocurrency, which resulted in serious charges being brought against its Australian promoter in November 2020 after its collapse.

The ACCC is also focused on cross-border investigations, with the Multilateral Assistance and Cooperation Framework for Competition Authorities coming into effect in September 2020. This agreement is between the ACCC and the equivalent bodies in the United States, United Kingdom, Canada, and New Zealand, and aims to increase cooperation between these agencies in the exercise of their surveillance and enforcement activities.

Financial crime issue predictions for 2022

Australia's active regulatory landscape means that companies operating in all sectors, and particularly those sectors identified as priorities above, should prioritise compliance and work quickly to address any areas of potential non-compliance that they identify.

Companies should ensure that their policies and procedures, including their AML/CTF programme, whistleblower policies, and modern slavery statements, remain up to date and foster a culture of compliance across the organisation.

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

Sarah Alawi
Associate – Sydney
Tel +612 9373 7673
sarah.alawi@allenovery.com

"The location of the team combined with having U.S. qualified and highly-experienced lawyers in the APAC region makes them an ideal choice for anything FCPA-related. The team communicates extremely well and are pragmatic in their advice and approach to complex investigations. They are flexible and open to finding solutions to manage their work in a cost-effective way."

"Great integration of all local legal requirements of our various subsidiaries into the final work product. Very good at adapting to the client brief and delivering an appropriate solution, nothing over-engineered."

Legal 500 Asia Pacific 2021

"Delivering fast turnaround times. Good listeners to the actual situation of the company and adjusting the process and output to the needs. Very pleasant to deal with."

Chambers Asia Pacific 2021

"Jason Gray is commended for his ability to advise on anti-bribery and corruption matters throughout the Asia-Pacific region, and is especially highlighted for his expertise in U.S. FCPA matters. Clients say: 'He is U.S.-qualified, which is fantastic. He knows the US regulations very well and can leverage that well on matters in the Middle East and Asia, leading a lot of investigations in Asia-Pacific and Europe.'"

Chambers Asia Pacific 2020

Belgium

Criminal enforcement in Belgium was robust in 2021, focusing on complex fraud and money laundering involving financial intermediaries, corruption, cybercrime, and environmental pollution. The Belgian legislator continues to develop a Business and Human Rights framework as an additional tool to sanction breaches of fundamental rights. Private companies are increasingly sensitive to criminal law risks, including in the field of M&A, where compliance in the broad sense of the word has become a focal point. Looking forward to 2022, we expect these trends to intensify. The implementation of the EU Whistleblowing Directive will result in increased disclosures, fuelling new investigations and criminal prosecution. Also under EU influence, the operationalisation of the European Public Prosecutors Office will elevate financial crime on the enforcement agenda, strengthen cross-border enforcement, and favour contentious litigation over out-of-court settlements.

Investigations trends/developments

EU Whistleblowing Directive will fuel more investigations

The new EU Directive on the protection of persons who report breaches of Union law (the **EU Whistleblowing Directive**) aims to protect whistleblowers when making an extensive range of disclosures on breaches of EU law, including in areas related to public procurement, financial services, the protection of the environment and public health.

In view of political calls in Belgium for an extensive scope of implementation (expanding it to *all possible breaches of law* at both the national and European level), and that protection is granted to a wide range of reporting persons, we expect an increasing number of disclosures and investigations by the Belgian authorities as a result.

Investigations by the Belgian authorities will also be fuelled by the fact that: (i) the EU Whistleblowing Directive obliges Belgium to install external whistleblowing reporting processes enabling the whistleblower to contact a competent authority directly; and (ii) protection under the EU Whistleblowing Directive is not conditional on the whistle-blower first reporting any breaches internally.

We also anticipate an increase in cases of improper use of whistleblowing procedures.

For more information on the EU Whistleblowing Directive see our eAlert and Global Benefits Vision issue 34.

The deadline for transposing the EU Whistleblowing Directive was 17 December 2021. However, Belgium (together with several other EU member states) has not met this deadline. At this stage, it is still unclear what the Belgian legislation transposing the EU Whistleblowing Directive will contain, especially in view of the advice issued by the Belgian National Labour Council on 30 November 2021 suggesting a number of material changes to the draft proposal of such legislation.

The governmental negotiations began in January 2022, but voting in the parliament is only scheduled for July 2022. Nonetheless, the European Court of Justice and Belgian courts and tribunals may rule that the EU Whistleblowing Directive has some direct effect. Belgian companies are therefore encouraged to assess how they will react to the EU Whistleblowing Directive prior to its Belgian implementation.

Impact of new European Public Prosecutor's Office

The European Public Prosecutor's Office (the **EPPO** went live on 1 June 2021. Since then, more than 300 investigations have been opened into alleged crimes contravening the EU's financial interests, including different types of fraud (notably VAT fraud, customs fraud, and fraud involving EU subsidies), money laundering, passive and active corruption, and the misappropriation of funds.

We expect that the EPPO's operationalisation will cause these types of crime to rise on the enforcement agenda in 2022. It will be interesting to see if the EPPO adopts a favourable approach to settlements (a preferred resolution mechanism in the Belgian enforcement practice toolkit), or whether more cases will be submitted to the courts.

The potential to reach settlements in EPPO investigations relating to customs matters is however limited, and an EPPO case cannot be dismissed solely at the authorities' discretion. The question of whether or not to settle will now be decided in Luxembourg instead of at the national level, and it is expected that larger cases involving higher damages will not be settled but submitted to the courts instead.

More information on the EPPO and its impact can be found in our first eAlert in a series on the subject.

Significant law reforms impacting corporate criminal liability

Business and Human Rights (BHR)-related liability throughout value chains

Further to calls for the EU to adopt mandatory corporate due diligence legislation, the European Commission and European Parliament have undertaken some preliminary steps in response. In line with the developments at EU level, the Belgian legislator introduced a legislative proposal on corporate vigilance and corporate accountability (the **Belgian Vigilance Proposal**) in April 2021, which is currently being discussed before the Belgian Parliament.

Three new legal instruments aim to establish a duty of vigilance requiring companies to: (i) respect human rights, labour rights and the environment; and (ii) identify, prevent, mitigate and cease environmental harm, human rights and labour rights violations, or any risks thereof, throughout their value chain.

The Belgian Vigilance Proposal envisages an extensive liability regime for breaching the duty of vigilance, including criminal sanctions, as described in our article of 4 May 2021. Non-compliance may give rise to fines of up to EUR1,600,000 for companies. While this proposal has not yet been adopted, it has been given considerable attention by the Belgian legislator, which is expected to follow the example of its French and German counterparts, thereby giving rise to enhanced liability risks for companies throughout their value chain.

Continued proliferation of sanctions as a tool of public policy, further increasing the compliance burden for private entities

Sanctions continue being used as a geopolitical tool, further increasing the compliance burden on companies (including in the face of conflicting policies adopted by the world's major blocs, including the EU and the U.S.). Notable examples include:

– additional listings under country-specific sanctions regimes (including Myanmar and Belarus) as well as under the standalone EU cyber sanctions regime (targeting individuals and entities suspected of involvement in cyberattacks; see our earlier eAlert here);

– the introduction of the EU's own human rights sanctions regime (targeting individuals and entities suspected of involvement in serious human rights violations or abuses), with the first designation and calls for more to follow; and

– a Belgian legislative proposal to introduce individual sanctions for serious human rights violations at the Belgian level, which would enable Belgium to act where the required unanimity rule acts as a brake at the European level.

We reported last year that the Belgian Ministry of Finance and Economy was empowered to impose administrative fines for breaches of EU sanctions, in addition to the already existing possibility of criminal prosecution. In Belgium, cases of actual enforcement of sanctions remain relatively scarce but, as part of an overall focus on financial crime, we expect an increased focus on this by Belgian prosecutors.

Data retention and the encryption debate

In a long-anticipated April 2021 decision that came after earlier decisions by the European Court for Human Rights, the Belgian Constitutional Court annulled the Belgian legal framework requiring telecom operators to store traffic and location data in bulk. Applauded by privacy advocates but widely criticised by law enforcement, the decision may affect evidence already gathered in ongoing criminal investigations, and it is argued that it will make the prosecution's task more difficult in the future.

In response, the Belgian federal government is currently considering new legislation that would continue to require bulk data storage in specific circumstances, and which some argue would undermine the use of end-to-end encryption in Belgium by de facto forcing the creation of encryption backdoors. This proposal will no doubt be the subject of intensive political and legal debate in the course of 2022.

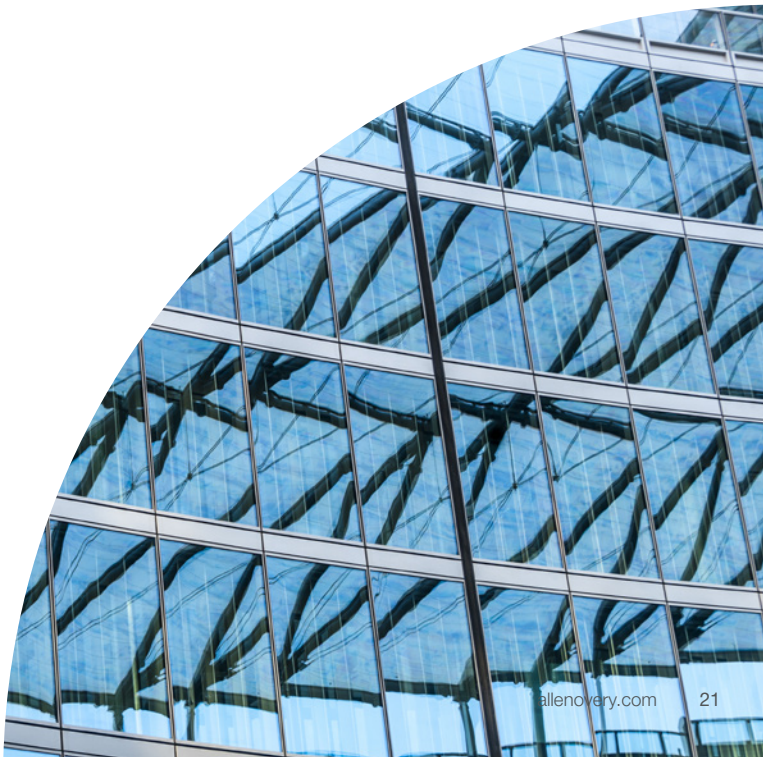
Internal investigation – key developments

Increased focus on "doing the right thing", and "being seen to be doing the right thing"

A number of developments have caused Belgian companies to increasingly consider conducting an internal investigation when compliance issues are reported and the manner in which they should proceed. This trend will accelerate following the adoption of the EU Whistleblowing Directive and its imminent Belgian transposition (see above).

Workplace investigations have become increasingly common due to a shift in society towards encouraging a professional "speak-up" environment, including the #metoo and #BlackLivesMatter movements. Belgian companies are actively introducing ESG principles into their corporate governance practices, and "doing the right thing" and ensuring a healthy workplace are becoming increasingly important from an employer-branding and investor-attraction perspective. Focusing increasingly on compliance, and investigating concerns through internal fact-finding investigations, Belgian companies are tending to turn to external law firms for strategic guidance, in an effort to ensure impartiality, compliance with applicable laws and preservation of legal privilege.

This trend is accelerated further due to the general public's increased expectation of transparency and voluntary disclosure, for example in the case of environmental pollution. Enforcement authorities are increasingly holding companies to account for a lack of transparency, even beyond the strict legal requirements. This, in turn, raises important questions concerning the preservation of legal privilege and the right against self-incrimination.



Sectors targeted by law reforms or enforcement action

Environmental pollution

There are more criminal investigations into environmental pollution, in the broad sense of the word, e.g. noise pollution, chemical spills, and air contamination have recently all given rise to enforcement action. Besides the authorities' own willingness to sanction these issues under criminal law, there has been an increase in the general public's vigilance of environmental pollution, as well as in (criminal) complaints being lodged by private individuals and advocacy groups.

Football sector

The Belgian football sector has been the specific focus of increased regulation (including by an extension of the Belgian AML Act) and has already been the subject of enforcement action. Specifically, Operation Zero, the widely publicised criminal investigation into various alleged offences, including private corruption and fraud by various first-division clubs and affiliated individuals, is expected to result in criminal prosecutions in 2022. This is the first application of the new Belgian legal framework for cooperating offenders, under which suspects assist the authorities in a criminal investigation in return for a reduced sentence.

Cybercrime

Accelerated by the global pandemic, cybercrime continues to increase and is becoming more and more sophisticated, opportunistic and methodical, with threat actors focusing on high-value targets, affecting entire supply chains and using cryptocurrencies to launder criminal proceeds. Against the background of the continued rise in cyber-enabled financial crime (in particular in online fraud, phishing, ransomware, and other means of cyber extortion, including DDoS-for-ransom), the Belgian authorities continue to focus on fighting cybercrime, often in international police operations coordinated by agencies such as Europol and Interpol, and to assist victims of cybercrime in responding to (including through the sharing of threat intelligence) and recovering from cyberattacks (including through the offering of operational support).

Cross-border coordinated enforcement activity

Cross-border enforcement activity under the impetus of the EPPO

The last few years have marked a significant increase in cross-border fraud investigations, coordinated at EU level by the European Anti-Fraud Office (**OLAF**). The introduction of the EPPO (see above) now means that a unique regime applies for cross-border cooperation within the EU. In EPPO investigations, prosecutors handling a case in one participating member state will be able to directly assign specific investigation tasks to prosecutors in other member states, which may increase efficiency. In Belgium, we expect an increase in customs-related cross-border investigations, with a focus on goods coming in through the port of Antwerp and with limited possibilities that such cases will be settled.

Internal investigations with focus on improper workplace conduct

There has been an uptick in internal cross-border investigations in the context of improper workplace conduct occurring in multiple jurisdictions, or that involve employees working in different jurisdictions. We expect this trend to continue, particularly in light of the adoption of the EU Whistleblowing Directive (see above).

Financial crime predictions for 2022

Preventing, detecting and responding to corrupt practices, money laundering, improper workplace conduct, and compliance with laws generally will stay high on the agenda of GCs in 2022, accelerated in particular by the imminent legislative protection of whistleblowers and the increased compliance pressure from a broad range of stakeholders. Organisations in all sectors will be expected to set up and implement internal reporting channels in line with prescriptive standards and will be exposed to an increased risk of litigation.

In M&A, we expect a continued focus on compliance as an integral part of any due diligence exercise, with particular focus on matters as diverse as anti-bribery and corruption, sanctions and embargoes, environment and human rights, workplace conduct, and data protection and cybersecurity.

Finally, as was the case previously, because of the opacity of money flows in complex cases and the focus on "deep pockets", we expect a continued focus by Belgian prosecutors on financial intermediaries when investigating and prosecuting fraud.

Key team members

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

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

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

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

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

Justine Tixhon
Trainee – Brussels
Tel +32 2 780 2640
justine.tixhon@allenovery.com

"A hands-on and available team, that never loses focus on key topics."

Legal 500 2020 (Belgium, Fraud and white-collar crime, Tier 1)

"The team is proactive and always thinking ahead."

Chambers 2021 (Belgium, Dispute Resolution, Tier 1)

"Still the number one firm for high-stakes litigation in Belgium."

Chambers 2020 (Belgium, Dispute Resolution, Tier 1)

"[Joost] Everaert is very thorough, his submissions are very detailed and complete, he makes sure nothing is missing."

Chambers 2021 (Belgium, Dispute Resolution)

Mainland China

New data protection and data security laws in China add considerably to the complexity of conducting cross border investigations with a nexus to China, and meeting information requests from foreign regulators. A new 'anti-sanctions' regime is aimed at counteracting foreign sanctions and trade controls, and multinational companies doing business in China are expected to follow it. The ABAC regime continues to develop with a greater focus on enforcement against private company offerors of bribes. The real estate and construction industries have been the primary focus of criminal actions in 2021, and the life sciences industry remains the primary focus of administrative penalties. We expect to see more enforcement actions in these areas in 2022.

Investigations trends/developments

Continuing efforts in the anti-bribery and anti-corruption (ABAC) campaign

2021 saw a substantial decline in the number of published criminal bribery cases, while the number of administrative penalty decisions increased slightly. China Judgments Online reported 104 first-instance bribery convictions through the end of October 2021, as compared to 492 convictions in the same period in 2020. The real estate and construction industries have accounted for nearly one-third of the cases in 2021.

The number of administrative penalty decisions for commercial bribery increased from 62 to 64 cases, with more than one-third of cases involving the life sciences industry.

Despite the fall in bribery prosecutions, the government has explicitly committed to expanding its anti-corruption campaign. Multiple authorities of the Communist Party of China (**CPC**) and the central government issued the *Opinions on Furthering Concurrent Investigations of Active and Passive Bribery* in September 2021. They are designed to foster inter-departmental cooperation, and reduce the traditional lack of coordination in handling passive and active bribery cases.

The opinions stated that more focus will be given to bribery that is:

- repetitive
- high value
- to multiple recipients
- in key national projects
- in the following areas:
  - organisation and personnel matters
  - law enforcement and judicial
  - environmental protection
  - finance
  - food
  - pharmaceutical
  - charity
  - social security
  - education
  - medical.

For multinational companies, an additional regulator must now be considered. The National Supervisory Commission (**NSC**), which previously had jurisdiction primarily over passive bribery cases, now has derivative jurisdiction over private-sector bribe offerors. The investigative procedures of the NSC are usually considered more rigorous than the normal criminal procedures. While normal criminal procedures allow a suspect to access an attorney after initial questioning, there is no access to an attorney in investigations by the NSC.

The consolidation and coordination of regulatory enforcement of bribery offences are likely to increase the number of corruption prosecutions, such that next year may well see a reversal in the significant drop in cases that we saw in 2021.

Increased liability for independent directors of listed companies

Listed companies in the PRC must have a board with more than one-third independent directors. Though independent directors are commonly less involved in the day-to-day business operations of a listed company, their liability is similar to those of other directors. Up until now, independent directors have rarely been held directly responsible, or only incurred supplementary liability for corporate misconduct, paying only insubstantial amounts after the persons with primary liability have settled their claims. The position of an independent director is in practice often perceived as "honorary" rather than that of a gatekeeper as intended by the legislator.

A recent ruling concerning the legal liability of independent directors has shone the spotlight on their exposure. On 12 November 2021, the Guangzhou Intermediate People's Court ruled that five independent directors of a PRC listed company, Kangmei, should be jointly liable for a combined RMB370 million, accounting for around 15% of the total losses suffered by investors due to financial fraud by some Kangmei executives and external accountants. For context, the remuneration for each of those independent directors is only around RMB100,000 per annum.

The strengthened scrutiny of independent director liability accords with PRC regulators' campaign in recent years to combat misrepresentation by issuers and due diligence failures by intermediaries. Directors and Officers Liability Insurance products in China are very limited so independent directors of PRC listed companies will be in an increasingly delicate position. Since the Kangmei ruling, more than 20 PRC listed companies have announced the resignation of their independent directors, with more likely to come. We expect that the liability of independent directors will become one of the many issues that must be considered in any future investigation of corporate misconduct.

Significant 2021 law reforms impacting corporate criminal liability

China's "Anti-sanctions" regime

In the context of increasing geopolitical tensions, China has introduced two significant tools into its regulatory toolbox:

– *Measures for Counteracting the Unjustified Extraterritorial Application of Foreign Laws and Measures* (**Blocking Rules**), a Ministry of Commerce regulation that took effect on 9 January.

– *PRC Anti-foreign Sanctions Law* (the **AFSL**), a law passed on 10 June.

Along with the *Unreliable Entity List Regulation* adopted in September 2020, the Blocking Rules and the AFSL more directly target foreign sanctions. They allow the Chinese government to nullify foreign sanctions, export controls and other perceived "discriminatory restrictive measures" (**DRM**s) that are considered harmful to China's sovereignty, security, or development interests, at least within the territory of China. The AFSL also provides the government with the legal basis for establishing a retaliatory sanctions programme targeting individuals and organisations responsible for such DRMs.

The Blocking Rules apply to foreign laws with extraterritorial application or measures that unjustifiably prohibit or restrict Chinese parties from engaging in normal economic, trade, and related activities with a third country (or region) or parties from that country, in breach of international law and the basic principles of international relations. Penalties for violating the Blocking Rules are, however, relatively limited, consisting mostly of administrative penalties for Chinese violating parties, and civil liability (i.e. monetary damages) for foreign violating parties.

The AFSL is far broader in scope. Pre-AFSL, the Ministry of Foreign Affairs (**MOF**) had announced a number of "ad hoc" sanctions against foreign individuals and organisations perceived to be hostile to Chinese interests. The AFSL now provides a clearer legal basis for such sanctions (called "countermeasures" in the law) and the mechanisms supporting their enforcement. Parties in the territory of China who breach the countermeasures may be subject to a restriction or prohibition of activities. Breaching parties outside of China face unspecified consequences ("shall be held liable according to law").

Similar to the Blocking Rules, the AFSL allows aggrieved Chinese parties to bring suits before Chinese courts against individuals or organisations that implement or assist the implementation of DRMs. The remedies include both damages and injunctive relief.

China's deployment of its new anti-sanctions regime, to date, has been relatively narrow in focus. At the same time, the new regime poses a range of challenges for multinational companies doing business in China, including how they negotiate contracts, how they audit or monitor their customers or supply chains, and how they engage generally with their Chinese counterparties.

Substantial expansion of China's data protection regime

China's nascent data protection regime has been substantially reshaped by the PRC Data Security Law (the **DSL**) and the PRC Personal Information Protection Law (**PIPL**), both of which were introduced in 2021.

Before the enactment of the two laws, the primary foundational data legislation in China was the *PRC Cybersecurity Law* (**Cybersecurity Law**). The Cybersecurity Law applies to the construction, operation, maintenance, and use of "networks", and the supervision and administration of cybersecurity within the territory of China. It requires "network operators" to: (1) establish and maintain sufficient processes and infrastructure to protect the security of their networks; (2) follow certain rules on their network activities, including in particular the collection and use of personal information; and (3) supervise the activities of users of their networks.

The DSL and the PIPL have changed the regulatory landscape of China's data regime. While there are still some disputes on the relationship between DSL, PIPL and the Cybersecurity Law, the legal community tends to agree that the DSL and the PIPL either supplement or supersede the Cybersecurity Law, and provide more onerous requirements in certain areas, particularly security preservation, cross-border data transfer and personal information protection.

The DSL applies to all "data processors" (undefined), and processors of "important data" and "core data" are subject to heightened requirements. The PIPL applies to all "personal information processors", including those foreign processors processing personal information for the purpose of providing products or services to individuals in China, or analysing and evaluating the activities of the same. After the enactment of the two laws, we have observed an acceleration in the promulgation of the supporting regulations.

Internal investigations – key developments

The DSL and the PIPL (see above) greatly add to the complexity of internal investigations, particularly where cross-border transfer of documents, evidence, and findings is involved.

Internal investigations typically involve the processing of employees' personal information. The PIPL requires, by default, that the processing of personal information be conditional upon a data subject's informed consent, and it is unclear if the statutory exceptions apply in the context of internal investigations. Even if the employer has procured general consent from its employees to process personal information in the context of internal investigations, by means of employment contracts or compliance certifications, nothing forbids the employees from withdrawing their consent and requesting deletion of any personal information collected. It is unclear if the law permits subjecting such withdrawals and orders to disciplinary action for failure to comply with an investigation. Notifying data subjects of processing is an obligation separate from procuring consent, with even narrower exceptions. Therefore, the law on its face appears to pose substantial challenges to conducting early-stage stealth investigations.

Another major concern is cross-border transfer of data:

– According to the DSL, export of "important data" collected or generated within the territory of China must be done in accordance with either the Cybersecurity Law (i.e. passing a security assessment) or state regulations. "Important data" is not defined in the DSL but there are some clues. Relevant factors include whether the data is important to economic and social development, and the degree of harm to national security or public interest if it were to get into the wrong hands. It is expected that regional and industrial regulators will establish catalogues of "important data".

– Under the PIPL, all cross-border transfer of personal information is subject to statutory restrictions, regardless of the importance or sensitivity of the information. The processor must procure "separate" informed consent from the data subject, and must take "necessary measures" to ensure that the activities of foreign recipients meet the protective standards prescribed in the PIPL. Certain "large scale personal information processors" must also pass government-organised security assessments. Other processors may have to: (1) obtain security certifications issued by government accredited agencies; (2) execute standard agreements (using government-issued templates) with foreign recipients; and (3) comply with other conditions in laws and regulations.

Restrictions on cross-border data transfer are even stricter where the transfer is in response to, or in the context of, data requests from foreign government authorities. The DSL provides, in summary, that no organisation or individual in China can give data stored in China to foreign judicial or law enforcement authorities without the approval of the competent authorities. A similar provision applies to personal information under PIPL. These new blocking rules are broader than similar restrictions in existing legislation and are accompanied by substantial penalty provisions to assist enforcement.

At present, there are no detailed implementation regulations defining the procedures on the security assessment, security certification, or government approvals mentioned above, and the template data security agreement that a data processor may need to execute with foreign recipients has not been issued. However, it is not a stretch to say that these data blocking statutes pose significant new challenges in foreign regulator facing investigations or enforcement actions.

Sectors targeted by law reforms or enforcement action

In the anti-bribery area, the real estate and construction industries have been the primary focus of criminal actions in 2021, and the life sciences industry remains the primary focus of administrative penalties.

Additionally, as discussed above, the Opinions expressly list a number of areas of focus, including the financial, food, pharmaceutical and healthcare, and education markets.

Cross border coordinated investigation or enforcement activity

Due to the pandemic and geopolitical conflicts, there has been no significant coordinated cross-border investigation or enforcement activity in 2021.

Financial crime predictions for 2022

In addition to existing blocking provisions, the DSL and the PIPL will add complexity to the cross border transfer of documents and evidence, particularly in the context of requests from foreign government authorities. The requirements for informed consent of data subjects impact how stealth internal investigations can practically be conducted in China.

The enhanced anti-sanctions measures introduced by the Chinese government pose challenges for multinationals doing business in China that must now cooperate with Chinese sanctions imposed on certain politicians and organisations within their home countries. Where foreign sanctions are impacted by the new Chinese laws, multinationals may also find themselves in a dilemma. While some efforts can be made to mitigate the risks from the conflict of laws, it can be difficult to forge a path which caters for compliance with all applicable laws concurrently.

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
Senior Associate – Shanghai
Tel +86 21 2036 7142
yihan.zang@allenovery.com

Jason Song
Associate – Shanghai
Tel +86 21 2036 7121
jason.song@allenovery.com

Eugene Chen "is a popular choice for clients facing investigations and enforcement actions brought by U.S. and Chinese regulatory bodies. He offers further expertise in handling corruption claims and advising on anti corruption strategy."

Chambers Asia Pacific 2020, Corporate Investigations/Anti-Corruption (International Firms), China

Jane Jiang "advises financial institutions and multinational corporations on regulatory questions arising out of their activity in China and abroad. She is well versed in investigations and cross-border litigation."

Chambers Asia Pacific 2020, Financial Services: Contentious Regulatory (International Firms), China

France

France remains a hub for white-collar crime enforcement. Spearheaded by the National Financial Prosecutor's Office (**PNF**), the white-collar criminal enforcement landscape continues to move towards greater collaboration with overseas enforcement authorities, corporate settlements, and heavy fines. The fight against money laundering, tax evasion and corrupt practices remains at the forefront of enforcement action, alongside a rising number of investigations in the area of Environmental and Social Governance (**ESG**). Several bills have been presented by MPs to the French Parliament over recent months, relating in particular to the fight against corrupt practices, the internal investigation process and the protection of whistleblowers. Depending on how they progress through the French Parliament, they may give rise to new obligations for corporates with a French nexus in 2022.

Investigations trends/developments

Criminalisation of ESG breaches

The criminalisation of companies' breaches of their Environmental and Social Governance (**ESG**) policies with regard to human rights is an emerging trend. In particular:

– An investigation was opened in July 2021 by the National Financial Prosecutor's Office (**PNF**, *Parquet national financier*) against several multinational groups in the textile industry, accused of benefiting from (*recel*) the proceeds of crimes against humanity perpetrated against Uyghurs in their Chinese subcontractors' factories.

– Two other complaints were filed in 2020 and 2021 against multinational groups. Plaintiffs argue that the violations of Uyghurs' human rights in Chinese subcontractors' factories amount to a breach of the ethical commitments of the multinational groups and therefore constitute misleading commercial practices (*pratiques commerciales trompeuses*).

– In October 2021, a French tech company was placed under formal investigation (*mise en examen*) for allegedly aiding and abetting torture and enforced disappearances, and selling cyber surveillance material to the regime of Abdel Fattah al-Sisi, which would have enabled it to track its political opponents.

A focus on tax evasion

2021 also saw a move towards enhanced prosecution of tax evasion. In the context of French-style deferred prosecution agreements (known as **CJIP**, *Convention Judiciaire d'Intérêt Public*), a foreign bank agreed to pay EUR25 million for aiding and abetting a tax evasion by issuing loans to the perpetrators of such tax evasion. New guidelines published by the Ministry of Justice in October 2021 intend to facilitate the exchange of information between prosecutors and the French tax authority in order to help prosecutors characterise the constituent parts of tax evasion. The PNF stated in mid-2021 that two-thirds of the French guilty plea procedures that it led (known as **CRPC**, *Comparution sur Reconnaissance Préalable de Culpabilité*) were related to tax evasion.

Offences against the EU budget

At the European Union (**EU**) level, the European Public Prosecutor's Office (**EPPO**) started its mission in July 2021 for the prosecution of offences against the EU budget, such as fraud, corruption and cross-border VAT fraud. The Paris section of the EPPO has taken on five cases out of the 40 complaints reported to the Paris section since July 2021, and intends to increase the volume of investigations in the upcoming years.

Significant law reforms impacting corporate criminal liability

A recent ruling by the French Supreme Court (*Cour de cassation*)[1] asserts that a company may be placed under formal investigation (*mise en examen*) for aiding and abetting a crime against humanity. The mere fact that the multinational company paid an organisation while it was allegedly aware of the organisation's purely criminal purpose is sufficient to characterise that the company aided and abetted such organisation. This ruling is likely to extend the scope of corporate criminal liability. French banks have already been subject to investigations for aiding and abetting crimes against humanity over recent years and the ruling will inevitably increase this trend.

Ongoing legislative reforms are likely to affect corporate criminal liability, although they may evolve during parliamentary debates:

– MP Sylvain Waserman presented a bill before the French National Assembly aimed at clarifying and enlarging the definition of whistleblowers, the scope of information considered to constitute a whistleblowing and the possibility for whistleblowers to use both internal and external reporting channels (bill of 21 July 2021 transposing the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report violations of Union law (**EU Whistleblowing Directive**)).

– MP Raphaël Gauvain presented a new anti-corruption bill (hereafter the **Sapin III bill**) before the French National Assembly on 19 October 2021, aimed at enhancing the French anti-corruption framework, notably the French Law No. 2016-1691 of 9 December 2016 (known as the **Sapin II Law**). In particular, it suggests extending the scope of the anti-corruption compliance requirements to the French subsidiaries of foreign parent companies.

A reform of the French judicial system, which is being reviewed by the French Constitutional Council (*Conseil constitutionnel*), has led to strong debates on the scope of attorneys' legal privilege in France. The bill explicitly recognises the existence of attorneys' legal advice privilege, aligned with legal privilege relating to the rights of defence. It also memorialises the inability of attorneys and their clients to rely on legal advice privilege where communications between them may have helped perpetrate or facilitate corruption, tax fraud and terrorist financing.

1_Cass. Crim., 7 September 2021, n° 19-87.367.

Internal investigations – key developments

The Sapin III bill proposes new provisions in the French Code of Criminal Procedure to strengthen the rights of individuals during an internal investigation. The proposed law provides, inter alia:

– New guarantees, directly inspired by the rights of persons in police custody, including notification of rights and reading of the interview transcript prior to signature.

– The right of an interviewee to have access to the criminal case file where there are reasonable grounds to suspect that he/she participated in the misconduct under investigation;

– The possibility for the Public Prosecutor, if a CJIP is being considered, to request the appointment of an ad hoc representative or a special committee to conduct the internal investigation. This provision is intended to avoid potential conflicts of interest that may arise in the event that certain directors are involved in the acts of which the entity is accused.

The French Anti-Corruption Agency (**AFA**, *Agence française anticorruption*) has published various guidelines this year on internal/external investigations:

– The new version of its Recommendations, published in January 2021, recommends that companies which are subject to the obligation to implement a compliance programme should define and formalise an internal investigation procedure.

– The practical guide on anti-corruption verifications in merger and acquisition transactions, updated in March 2021, recommends that internal investigations be conducted (by the buyer or the seller, depending on the situation) at the level of the target company.

– The guide to preventing conflicts of interest in companies, published on 18 November 2021, encourages the reporting of any conflict of interest situation, which could lead to an increase in internal investigations.

– The draft practical guide on anti-corruption accounting controls in companies provides that in the event that a discrepancy flagged by such a control highlights suspicions or facts about corruption, this must be brought to the attention of the compliance officer and the management body, which may decide to conduct an internal investigation.

The French bill transposing the EU Whistleblowing Directive goes beyond the provisions of the Directive and could, if adopted, lead to an increase in whistleblowing and subsequent internal investigations.

Sectors targeted by law reforms or enforcement action during 2021

The economic sectors at risk of being investigated by the PNF remain those targeted by the so-called "Belloubet Circular" (published June 2020), namely: construction, mining, transportation, telecommunications, pharmaceuticals, energy and military equipment.

The French regulatory authorities will continue to focus their efforts on compliance with AML/CTF and corruption regulations by the financial services sector, including financial institutions, payment service providers and accountancy firms.

The AFA, which is responsible for ensuring that companies comply with their obligation under the Sapin II Law to implement anti-corruption systems and controls, could focus its inspections on:

– the public sector, where the implementation of anti-corruption measures remains weak according to the parliamentary information report intended to assess the impact of the Sapin II Law. In response to this finding, the Sapin III bill provides for the transfer of the AFA's advisory and control functions for public actors to the High Authority for the Transparency of Public Life (**HATVP**, *Haute Autorité pour la transparence de la vie publique*).

– the sports sector, given the economic stakes it represents and the recent scandals surrounding the awarding of competitions and within international federations, which have highlighted the need to adopt specific anti-corruption measures in this field.

Cross border coordinated investigation or enforcement activity

Although no coordinated CJIPs were reached in 2021 between the French authorities and their foreign counterparts, there is still a strong willingness amongst French criminal authorities to nurture cross border coordinated investigation and enforcement activity.

In June 2021, the head of the PNF affirmed to the French press that 80% of the investigations conducted by the PNF have an international component and that the coordinated CJIP between Airbus, the PNF, the U.S. Department of Justice and the Serious Fraud Office constituted a turning point in international cooperation.

As early as 2020, the PNF was getting ready to create "optimal cooperation" with the EPPO. According to the impact assessment conducted with respect to the bill on the EPPO and specialised justice, between 60 and 100 cases dealt with each year by the PNF, the inter-regional specialised criminal authorities and customs authorities could be referred to the EPPO.

Financial crime predictions for 2022

The French financial and banking industries are likely to continue to be key targets of enforcement action, with an increasing level of fines and penalties.

The fight against corruption is likely to remain a hot topic. Should the Sapin III bill succeed through the French Parliament, the French subsidiaries of foreign parent companies will have to conduct a gap analysis between their existing anti-corruption programmes and the anti-corruption requirements set out by French law.

The number of ESG-related investigations is likely to increase, with the protection of human rights and the environment being at the forefront of debates. Under French law, alleged victims and certain associations have the power to force the opening of a formal investigation, even if a public prosecutor considers that it is not worth pursuing the issue.

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

Marine Gourlet
Associate – Paris
Tel +33 1 40 06 53 47
marine.gourlet@allenovery.com

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

Louis Falgas
Juriste – Paris
Tel +33 1 40 06 51 47
louis.falgas@allenovery.com

"Allen & Overy LLP team consists of a deep bench of specialists who are able to cover criminal, financial, regulatory and commercial expertise which makes the practice particularly suited to complex hybrid cases. The team's caseload is very diverse and goes beyond the financial world: spanning insider dealing case, fraud, market abuses, corruption, money laundering, industrial, employment law and art-related criminal files. Several high-profile French companies have chosen the firm for high-stakes tax fraud, money-laundering, market abuse and unfair commercial practices cases."

Legal 500 EMEA 2021 – France (Dispute resolution: White-Collar Crime)

"Denis Chemla is an outstanding professional. He is always present, proactive and on top of matters. He is a pleasure to work with."

Legal 500 EMEA 2021 – France (Dispute resolution: White-Collar Crime)

"Dan Benguigui's expertise in handling combined complex white-collar crime and regulatory enforcement cases stands out."

Legal 500 EMEA 2021 – France (Dispute Resolution: White-Collar Crime)

"Hippolyte Marquetty enters the rankings following praise from the market. He regularly represents leading financial institutions, as well as corporates and private individuals. His expertise spans tax evasion, international corruption and fraud cases."

Chambers Europe 2021 – France (White Collar Crime)

Germany

2021 yielded many developments in the field of white-collar crime enforcement and investigations in Germany. In July, the German Federal Court of Justice (*Bundesgerichtshof*) ruled that obtaining a refund of unlevied withholding tax in connection with a cum/ex trade constitutes the criminal offence of tax evasion. Against this backdrop, criminal enforcement against participants in these trades continued unabated, with several dawn raids being conducted and new bills of indictment being issued. Criminal proceedings into cum/ex trading are now directed against more than 1000 suspects, including C-level executives of international banks.

In addition, the German legislator enacted a Supply Chain Due Diligence Act, which will come into force on 1 January 2023. The German lawmaker also expanded the scope of the criminal offence of money laundering with effect from 18 March 2021. The Corporate Sanctions Act, which was supposed to introduce more severe corporate fines and new rules for conducting internal investigations, was not passed. The previous German federal government also failed to enact the Whistleblower Protection Act, despite EU member states being obliged to transpose the underlying EU directive into national law by 17 December 2021. The new German federal government has announced that it will readopt these unfinished legal initiatives.

Investigations trends/developments

The German criminal prosecution authorities can be expected to continue their enforcement activities relating to cum/ex trades in 2022. We expect a wave of new indictments following the German Federal Court of Justice's decision on the illegality of cum/ex trades and the recent increases in human resources in both criminal prosecution authorities and criminal courts. In June 2021, a former senior banker was sentenced to five and a half years' imprisonment for his involvement in cum/ex trades. In addition, criminal courts have ordered the confiscation of proceeds generated by these trades, in one case resulting in a confiscation order of more than EUR176 million against a German bank.

There is an increased risk to companies and their managers of being confronted with allegations of business human rights infringements, which may even amount to accusations of participating in crimes against humanity. In September 2021, a non-governmental organisation filed criminal complaints against the managers of various fashion companies and retailers, accusing them of aiding and abetting crimes against humanity. The fashion companies or retailers have allegedly benefitted from forced labour by manufacturing or selling products containing cotton harvested in the Chinese province of Xinjiang.

Significant law reforms impacting corporate criminal liability

We expect a rise in the number of reports of suspicious activity and criminal investigations into alleged money laundering as a result of the changes made to the definition of criminal property. In March 2021, a legislative amendment to the criminal offence of money laundering (Section 261 of the German Criminal Code) came into force. Prior to the amendment, Section 261 of the German Criminal Code specified predicate offences for money laundering, thereby excluding the proceeds of various criminal offences such as theft, fraud and embezzlement, unless committed commercially (*gewerbsmäßig*) or by members of a gang. In contrast, under the revised provision, any criminal act can be a predicate offence for money laundering.

As of August 2021, the amended German Money Laundering Act (*Geldwäschegesetz*) requires all companies domiciled in Germany to provide detailed information on their ultimate beneficial owners to the German Transparency Register (*Transparenzregister*) within certain time limits. The German Federal Office of Administration (*Bundesverwaltungsamt*) is likely to continue its rigorous investigation and enforcement of contraventions of the transparency requirements.

The Supply Chain Due Diligence Act (*Lieferkettensorgfaltspflichtengesetz*), enacted in June 2021, aims to prevent human rights violations in supply chains. With effect from January 2023, companies operating in Germany and employing a certain number of employees will be subject to an entirely new set of rules obliging them to review their supply chains and to enact a supply chain-related compliance management system. The new rules demand remediation measures and may even require companies to terminate relationships with suppliers as a measure of last resort. The possibility of private enforcement measures by workers' unions and non-governmental organisations will further increase the exposure of companies to litigation, financial and reputational risks in connection with the new rules.

The new German federal government plans to reform the legal regime for corporate sanctions according to its coalition agreement. The government is also required to transpose the EU Whistleblower Directive into national law in the short term as the directive's deadline for implementation lapsed on 17 December 2021. A previous draft bill prepared by the former German federal government provided, among other things, that all companies with 50 or more employees and companies with an annual turnover of EUR10 million or more will be obliged to set up internal whistleblowing systems for employees.

Internal investigations – key developments

The German Federal Labour Court (*Bundesarbeitsgericht*) has acknowledged that a company can reclaim the costs of an internal investigation conducted by an external law firm from an employee under certain circumstances. It applied principles from previous case law, on the reimbursability of investigation costs in cases of suspected misconduct by employees, to the reimbursement of attorney fees. However, the Court set out strict requirements for such a recourse claim that will have to be taken into account right from the start of any investigation.

The Corporate Sanctions Act, by which the former German federal government planned to introduce new rules for conducting internal investigations, was not enacted. However, according to its coalition agreement, the new German federal government plans to create a "precise legal framework" for internal investigations. Some laws enacted by the previous German federal government, such as the Supply Chain Due Diligence Act, include features that were in the aborted draft Corporate Sanctions Act. This includes the mitigation of a corporate administrative fine in return for a company's efforts to uncover infringements of legal obligations.

Sectors targeted by law reforms or enforcement action

After a corruption scandal emerged involving several members of the German Federal Parliament (*Bundestag*) who had conducted business regarding medical face masks during the pandemic, the relevant criminal offence of bribery of elected officials (Section 108e of the German Criminal Code) has been increased to a felony with a minimum term of imprisonment of one year.

More than one hundred criminal investigation proceedings against operators of Covid 19 test centres are ongoing throughout Germany. The German federal government has already spent several billion euros on providing free lateral flow tests that were performed in these centres. Several operators are now being accused of fraud. In one case, the operator of more than 50 test centres nationwide is accused of having issued fraudulent invoices amounting to a total of more than EUR25 million. As a result, the German Ministry of Health issued a regulation to counter such fraud.

As a result of the *Wirecard* scandal, the German Federal Financial Supervisory Authority (**BaFin**) has been restructured and reorganised. Around 150 new positions have been created and a new head has been appointed, Mark Branson, the long-time director of the Swiss Financial Market Supervisory Authority. In addition, its competence in supervision and examination has been strengthened, and as a result BaFin now has the right to audit all capital market-oriented companies, not only banks, and is steadily gaining influence.

Cross-border coordinated enforcement activity

The highly controversial cum/ex transactions took place not only in Germany but throughout Europe. German criminal prosecution authorities are said to have set up joint investigation teams with their counterparts in other European countries.

Financial crime issue predictions for 2022

We expect a rise in criminal investigation proceedings into allegations of money laundering following the amendment of Section 261 of the German Criminal Code. We also anticipate that enforcement actions into requirements stipulated by the German Money Laundering Act, such as notification requirements vis-à-vis the German Transparency Register, will remain at a high level.

We expect a large number of high-profile indictments and criminal trials into alleged tax evasion in connection with cum/ex transactions in 2022. The proceedings will keep public prosecution authorities and criminal courts busy for years to come. The Regional Court of Bonn has even set up additional criminal chambers to handle the upcoming amount of cum/ex proceedings.

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
Counsel – Frankfurt
Tel +49 69 2648 5996
tim.mueller@allenovery.com

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

Laura Jung
Associate – Frankfurt
Tel +49 69 2648 5858
laura.jung@allenovery.com

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

"Wolf Bussian and Jan Erik Windthorst both have strong expertise in internal investigations in the financial sector."

Legal 500, Germany 2020

"[Jan Erik Windthorst] provides smart and clear legal advice."

Juve Handbook 2020/2021

"[Dr Tim Nikolas Müller] is very smart and always focused on the client's interests."

Juve Handbook 2021/2022

Hong Kong SAR, China

Personal data laws were amended in Hong Kong in 2021, meaning that businesses will need to be particularly careful about the expanded investigation and enforcement powers of the Privacy Commissioner for Personal Data (**Privacy Commissioner**). Despite Covid-19, financial regulatory enforcement actions have regained momentum. The Securities and Futures Commission (**SFC**) continues to focus on "high-impact" cases against financial institutions, listed companies and senior executives, with a targeted approach to enforcement. The Hong Kong Exchanges and Clearing Limited's (**HKEX**) enforcement agenda and power, as along with the Financial Reporting Council's (**FRC**) enforcement actions, have become more advanced and proactive. Various local regulators have increased their level of collaboration to combat corporate fraud, misconduct, and malpractices in the financial market.

Investigations trends/developments

The total number of actions commenced by the SFC declined from 2015 to 2019, and remained low from April 2020 to March 2021 (the **2020/2021 Period**). Nonetheless, the SFC appears to have regained some momentum despite the Covid-19 pandemic; the number of Securities and Futures Ordinance (**SFO**) section 179 inquiries[2] has increased by 35%, while there was a modest (3.6%) increase in the number of investigations started by the SFC compared to the previous financial year.

The cost of disciplinary fines has continued its upward trajectory since 2015. In the 2020/2021 Period, the SFC disciplined 31 corporations/individuals, with a combined value of fines levied reaching HKD2.81 billion. The value of fines rocketed to a historical high as a result of the SFC's record fine of HKD2.71 billion against a single financial institution for multiple rule breaches. The SFC sees this as an example of a "high-impact" case which poses risks to the investing public because of serious lapses and deficiencies in management supervisory, risk, compliance and anti-money laundering (**AML**) controls. In general, the SFC continues to focus on such "high-impact" cases.

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. Three former directors of a company (in the time-piece and jewellery industry) previously listed on the Stock Exchange of Hong Kong Limited (**SEHK**) were disqualified for between six and nine years for their respective roles in the company's misapplication of funds. The SFC also obtained compensation orders under the SFO against these three individuals for HKD622 million to compensate the company.

The SFC is also focused on investigating and eradicating "ram and dump" scams. These schemes occur where perpetrators corner a listed share, drive the share price up, and then use messaging applications and other social media platforms to induce unrelated investors to purchase the shares at the inflated price, before finally dumping all remaining shares in the market.

2_Section 179 empowers the SFC to compel the production of records and documents from persons related to a listed company in relation to fraud or other misconduct.

The HKEX's enforcement actions from late 2020 to mid-2021 focus on cases involving a failure to provide proper disclosure. In the six months ended 30 June 2021, the number of enforcement cases handled by the HKEX had increased by 55.7% compared to the same period in 2020.

In May 2021, the HKEX published revised Listing Rules, which include revised sanctions. There is a new director unsuitability statement and additional circumstances where disciplinary sanctions can be imposed. The implementation of these changes means that disciplinary action can be brought against a broader range of individuals, including members of senior management, if they cause or knowingly participate in a contravention of the Listing Rules. Overall, the amended Listing Rules strengthen the SEHK's power to hold accountable, and impose appropriate sanctions on, individuals responsible for misconduct and Listing Rule breaches.

For more analysis, see Hong Kong SFC's recent regulatory enforcement trends.

Significant law reforms impacting corporate criminal liability

Various amendments were made in 2021 to the Personal Data (Privacy) Ordinance (**PDPO**). Corporations therefore should adopt or update existing personal data policies and procedures, including handling notices from, and investigations by, the Privacy Commissioner, in order to ensure the new investigation powers are managed appropriately.

The Privacy Commissioner received new powers to pursue investigations, including in respect of suspected offences regarding disclosure of personal data without consent. The Privacy Commissioner can now (i) require materials and assistance from any person; (ii) apply for court warrants related to premises and electronic devices; (iii) stop, search and arrest persons without warrant; (iv) apply to a magistrate for a warrant to access, detain, decrypt and search for any materials stored in an electronic device that the Privacy Commissioner reasonably suspects to be or to contain evidence for the investigation; and (v) apply to the court to grant an injunction to prevent an offence.

Persons who, without reasonable excuse, fail to comply with the Privacy Commissioner's document requests, provide false or misleading information, or obstruct, hinder or resist the exercise of the powers to search and arrest are liable for an offence.

Two new criminal offences related to doxxing acts (non-consensual disclosure of an individual's personal information to harass or intimidate) were introduced. The Privacy Commissioner can require a person to cease or restrict disclosure of personal data within a specified timeframe if (i) there is non-consensual disclosure which contravenes any of the doxxing offences and in which the data subject is a Hong Kong resident or is present in Hong Kong at the time of disclosure; and (ii) a Hong Kong person or a non-Hong Kong service provider (for electronic messages) is able to take a cessation action (whether or not in Hong Kong) in relation to the message. The cessation notice has extraterritorial reach. Non-compliance is a criminal offence, with a fine of HKD50,000 and two-years' imprisonment for a first conviction, unless a statutory defence applies.

See Hong Kong's personal data law given new teeth – what they mean for businesses.

Internal investigations – key developments

A number of developments this year affect how a company should conduct an internal investigation.

The Hong Kong Monetary Authority (**HKMA**) released its consultation conclusions on the proposed Mandatory Reference Checking Scheme (**MRC Scheme**) in May 2021. The HKMA concluded that authorised institutions (**AIs**) will be required to obtain references, from current and former employers, of applicants who are directors and bank employees in senior management positions. AIs will need to (i) consider how to respond to reference requests while investigations are ongoing; and (ii) maintain sufficient internal employee disciplinary records on an ongoing basis so that they can easily provide information to the requesting AI. Issues will also arise as to how an AI should update a reference previously given following conclusion of an internal investigation that has raised questions over the fitness and properness of the departed employee.

The National Security Law (**NSL**), which came into force in 2020, states that a person who "*unlawfully provides State secrets or intelligence concerning national security for a foreign country or an institution, organisation or individual outside … the People's Republic of China shall be guilty of an offence*" (Article 29). There is currently little meaningful guidance on whether and, if so, how corporations may fall subject to this offence when dealing with cross-border investigations and foreign regulators or authorities, including how such information could be lawfully shared. However, a corporation should be vigilant when conducting investigations and communicating with foreign regulators or authorities in respect of the same to ensure that information or data that may concern national security is not unlawfully shared in contravention of the NSL.

For listed companies, the HKEX's new enforcement procedures demonstrate a clear need for comprehensive contemporaneous records to be maintained to address any queries the enforcement division may raise in the future regarding the company's business. The HKEX's new policy statement provides that its investigations will involve "*inviting written submissions from listed issuers, directors and other relevant parties to explain what has happened and their conduct, and to provide relevant information and documents*". As a result, listed issuers should ensure that they carry out internal investigations and prepare written records properly to facilitate provision of submissions and information to the HKEX. Regulators in Hong Kong acknowledge that legal professional privilege (**LPP**) is a fundamental right, although when dealing with the HKEX, a listed company may wish to waive LPP (on a full or limited basis) to gain credit for cooperation.

One of the HKEX's latest enforcement priorities includes "controls and culture". The implementation of appropriate controls, systems and culture involves ensuring the proper keeping of books and records. Enforcement investigators often request documentary evidence of steps taken by individuals and listed issuers to discharge duties and comply with the Listing Rules. The absence of such evidence will call into question whether those steps have been taken, the adequacy of the listed issuer's controls and compliance culture, and whether duties have been properly discharged.

For more analysis see:

– Hong Kong's proposed Mandatory Reference Checking Scheme: the end of "rolling bad apples"?

– Hong Kong's personal data law given new teeth – what they mean for businesses

Sectors targeted by law reforms or enforcement action

The HKEX's enforcement actions in 2021 against listed corporations and/or its senior management have been in a mix of industry sectors. Those industries include renewable energy, telecommunications, electronic products, and food and beverages.

During the 2020/2021 Period, the number of new listing applications decreased by 15.2% from 2019/2020, marking the lowest number of applications in any one financial year since 2017/2018. Nonetheless, the SFC continues to seek information from or express concerns with respect to listing applicants, using its regulatory powers under the Securities and Futures (Stock Market Listing) Rules. Specifically, in the 2020/2021 Period, the SFC directly intervened in 10.5% of the total number of listing applications, where it was aware of potentially serious disclosure or public interest issues. This is a slight drop in percentage from 2019/2020.

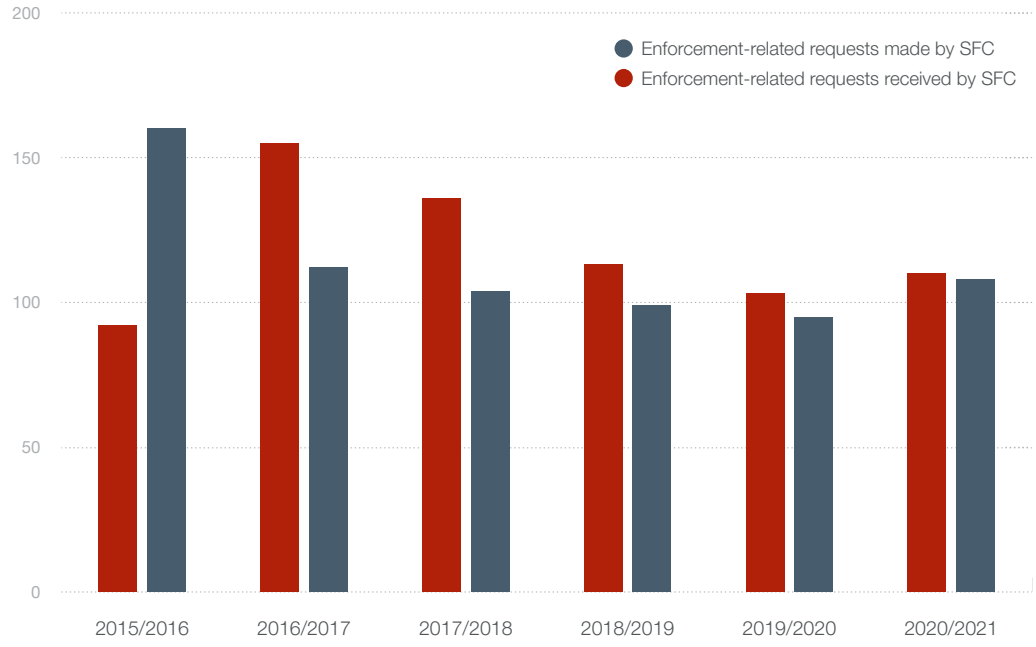
The Cyberspace Administration of China (**CAC**) released a draft regulation, the **Network Data Security Management Regulations**, for consultation. The draft regulation provides that "*data processing entities seeking a listing in Hong Kong that will influence or may influence national security*" must apply for a cybersecurity check. The draft regulation also shows an increasing focus by mainland authorities on the need to control the dissemination of data that may impact national security and, if implemented as drafted, will impose a new regulatory hurdle for Mainland-Chinese corporations seeking to list in Hong Kong.

Cross-border coordinated enforcement activity

The SFC maintained close enforcement cooperation with the China Securities Regulatory Commission (**CSRC**) during the 2020/2021 Period. In particular, the SFC, the Commercial Crime Bureau (**CCB**) of the Hong Kong Police, the CSRC and the Securities Crime Investigation Department (**SCID**) of the PRC Ministry of Public Security met in December 2020 to discuss collaboration in combating cross border securities crime.

There has been a slight increase in enforcement-related requests received and made by the SFC in the 2020/2021 Period compared to the previous year. This trend will likely intensify, given the application of PRC laws within Hong Kong.

Requests for regulatory cooperation



Financial crime issue predictions for 2022

Increased collaboration

We expect increased collaboration between regulators. In-house legal and investigation teams/GCs of financial institutions and corporations should stay vigilant as regulators conduct investigations from multiple aspects, such as misconduct, fraud, and corruption, while liaising together and sharing information obtained.

For example, the SFC and the Independent Commission Against Corruption (**ICAC**) have increased their collaboration by conducting joint operations to combat corporate fraud and misconduct of listed companies, directors or shareholders. The SFC and the CCB have also collaborated, including by conducting a joint operation against a listed company and its former senior executives suspected of a series of corporate fraud-related offences involving a total of HKD450 million.

In addition, in the 2020/2021 Period, the SFC signed memoranda of understanding (**MoU**) respectively with various local regulators. These include:

– an MoU with the FRC, a regulator focusing on auditors of listed entities, to strengthen the regulation of capital markets and foster closer cooperation in case referrals, joint investigations and information exchange;

– an MoU with the Competition Commission to enhance cooperation and the exchange of information; and

– an MoU with the Insurance Authority, which covers information sharing, case referrals and joint inspections and investigations.

Enforcement actions of FRC

We expect the Financial Reporting Council (FRC) to become increasingly active in its enforcement agenda. Since its establishment in 2006, it has become significantly more proactive in its enforcement actions. For example, it has commenced an investigation regarding the adequacy of reporting on a going concern (i.e. a company that has the resources needed to continue operating indefinitely until it provides evidence to the contrary) in China Evergrande Group's accounts and its auditor reports, and it recently conducted a joint search of an auditor alongside the ICAC following suspicions of misconduct and bribery.

In-house legal teams of listed entities will likely remain focused on the FRC's enforcement actions, the need to ensure compliance by its auditors, and the risk of being brought within an investigation by the FRC.

Anti-Foreign Sanctions Law (AFSL)

The AFSL in the PRC provides a framework in response to foreign sanctions, import prohibitions and export control restrictions. Under the AFSL, PRC government departments may impose countermeasures against individuals or organisations on a counter list, similar to the US government's Specially Designated Nationals and Blocked Persons List. The AFSL may apply to parties within or outside of China, having extraterritorial effect.

It seems clear that the AFSL will in some form and at some date be applied in Hong Kong, although according to the Hong Kong government, the PRC government does not have a timetable for doing so, and it is unclear whether the AFSL will be incorporated into Hong Kong law via local legislation or promulgation.

Nevertheless, as and when the AFSL is incorporated in Hong Kong as anticipated, financial institutions and corporations which implement and abide by US sanctions in Hong Kong may then be exposed to domestic legal risks.

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**."

– Legal500 Asia Pacific 2021, Hong Kong, Regulatory

Netherlands

The Covid-19 pandemic has resulted in fewer criminal enforcements in the Netherlands. Nevertheless, corruption and other types of economic and financial crime remain high priorities for the Dutch enforcement authorities. The Dutch regulators and the Dutch Public Prosecution Service (the **DPPS**) continue to pay close attention to supervised gatekeepers of the financial system for non-compliance with Anti-Money Laundering (**AML**) regulations and sanctions law. In cases where a legal entity enters into a settlement with the DPPS, there seems to be an increased focus on the prosecution of individuals. In the criminal tax field, in 2022 we expect more attention to be given to matters where the integrity of the financial sector is under scrutiny, such as dividend stripping. Cybercrime is high on the enforcement agenda. We also expect more cases that will relate to business responsibility for human rights. A follow-up to the legislative processes surrounding a draft bill related to judicial review of high-value settlements with the DPPS is expected.

Investigation trends/developments

More action against financial gatekeepers

Enforcement action against the gatekeepers of the financial system, such as banks, accountancy firms and notaries, for breaches of the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (the **AML Act**) continues to increase. Financial institutions have a growing role to play in the detection of money laundering, and risk criminal liability if they do not comply with the AML Act.

Financial intermediaries continue to be a target in (criminal) tax investigations. For example, the DPPS has started an investigation into the role of a large Dutch financial institution in a tax case, due to its involvement in certain dividend-related transactions. In addition, the Secretary of State for Finance has recently announced that tackling dividend stripping is proving to be difficult in practice, despite the existence of an anti-abuse provision under Dutch tax law since 2001. However, the Secretary of State also announced that the Dutch government is working on alternative measures using data available from five Dutch authorities, including the Dutch Fiscal Information and Investigation Service (the **FIOD**), the Financial Intelligence Unit of the Netherlands (the **FIU NL**) and the DPPS, in order to tackle dividend stripping more effectively from 2022 onwards. The public disclosure of the cum/ex Files by an international partnership of journalists seems to be contributing to a further focus by the Dutch Tax authorities on the recovery of taxes from taxpayers. This may also lead to criminal investigations into cum/ex trades by the DPPS.

A focus on individuals

The DPPS has become more focussed on individuals in cases where a legal entity has already settled with the DPPS. This trend is in line with the DPPS's 2020 instruction on high-value settlements, which urges caution when deciding not to prosecute a natural person when a legal entity has entered into a high-value settlement with the DPPS. Under Dutch law, persons who have actual control of the prohibited conduct committed within a legal entity can be held liable for this conduct.

Mediation being considered for criminal cases

Mediation as alternative dispute resolution is playing an increasing role in the Netherlands. The 'Innovation Act Criminal Procedure', a draft bill submitted to the Dutch Parliament in June 2021, contains the provision for a criminal case to be referred to mediation by a prosecutor or judge. Meanwhile, the feasibility of mediation as alternative dispute resolution in tax cases has been receiving increasing attention in Dutch political discussions. We expect the increasing recognition of the role of mediation to extend to complex fiscal fraud cases in the near future. Mediation in tax cases would help both the taxpayers and the Dutch Tax authorities in the continuation of their relationship after the settlement of their dispute.

Discouraging ransom payments for cyber attacks

Cyber attacks have increased in frequency and severity and have impacted multiple Dutch government organisations, knowledge institutions and corporates in recent years. 'Cybercrime as a service' is a phenomenon that seemed to be on the rise during the pandemic. As a result, the Dutch government and enforcement authorities are searching for effective methods to track down and prosecute cybercrime. They have advised against paying a ransom in the event of a ransomware attack because a ransom offers no guarantee of data being decrypted and, they say, perpetuates the criminal model. We expect to see an increased focus by the Dutch Data Protection Authority on data loss from cyberattacks. Compliance officers should ensure incident readiness and response to minimise the impact of data loss.

Significant law reforms impacting corporate criminal liability

AML

The EU published four legislative proposals relating to AML and efforts to combat the financing of terrorism (**CFT**) in July 2021, including:

– The creation of a new EU authority to improve the supervision of AML and CFT in the EU and cooperation among FIUs,

– Introducing an EU AML/CFT regulation – this would have direct effect, unlike the current EU AML directives which are required to be implemented in national law.

We expect that the focus on AML and CFT will continue and that the European legislative proposals will lead to domestic AML/CFT law reforms in the next few years.

Enhanced scrutiny of corporate settlements

High-value settlements with the DPPS have been a topic of discussion for years, due to, among other things, the lack of transparency, legitimacy and social acceptance of the criminal settlement process. In response, the Ministry of Justice and Security published a draft bill, which proposes judicial review for high value settlements. Since September 2020 a proposed high value settlement between a company and the DPPS has been reviewed by a committee consisting of a former lawyer, a former judge, a professor of criminal law and criminal procedure and former public prosecutors. This committee hears the views of the DPPS, the company and its counsel behind closed doors, and subjects the proposed settlement to a limited review only. The proposed draft bill imposes an obligation on the public prosecutor to hear the company with the assistance of a lawyer before making a preliminary offer of a high-value settlement. In addition, a written record of the hearing must be made and form part of the judicial review.

Environmental crime

The draft coalition agreement drawn up by the two largest political parties in the Netherlands in the summer of 2021 sets one of the objectives of the coming government as tackling environmental crime and environmental risks. The two political parties have called for a strong system of permit granting, supervision and enforcement, as well as sufficient enforcement capacity. We therefore expect an increased focus on compliance with environmental laws and regulations.

Ultimate beneficial ownership

A draft bill on the ultimate beneficial ownership (**UBO**) of trusts and similar legal arrangements was introduced in November 2021, which obliges entities to maintain and centrally register UBO information. The legislation implements the Fifth Anti-Money Laundering Directive (EU) 2018/843 (**AMLD5**).

Export control

A new European regulation on dual-use goods came into force on 9 September 2021, introducing several new rules and definitions. For example, cyber surveillance items are now subject to export control when they may be intended, in their entirety or in part, for use in connection with internal repression, and the commission of serious violations of human rights and international humanitarian law. In addition, the European regulation harmonises rules applicable to certain services with regard to dual-use items currently regulated at national level, such as technical assistance, and strengthens the cooperation between EU member states in the area of the enforcement of export control regulations. It is important for the compliance officers of exporting companies to scrutinise their framework on compliance with all new rules and responsibilities under the new European regulation.

Internal investigations – key developments

Lawyers and internal investigations

A rule of conduct for lawyers involved in internal investigations was clarified by the general council of the Netherlands Bar (Nederlandse Orde van Advocaten, NOvA) in May 2021. This clarification follows years of public debate on the role of a lawyer in an independent internal investigation conducted before or after an external authority has become involved. The NOvA clarified that lawyers can carry out internal investigations without breaching professional conduct rules. This is in line with our view that lawyers can conduct a proper fact-finding exercise, whilst at the same time acting in the best interest of their clients.

Privilege

There is public debate in the Netherlands regarding the scope of legal privilege in tax investigations. A draft bill proposes that the legal privilege of lawyers and civil-law notary only covers 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. This would mean, for example, that any communication regarding tax advice that is not directly linked to the aforementioned activities would fall outside the scope of legal privilege if information is requested by the Dutch tax authorities. The draft bill was met with criticism, including from the Dutch Bar Association and the Royal Notarial Association. Critics believe that, if the draft bill passes into law, this would erode legal privilege. The legislative process surrounding this draft bill is currently at a standstill.

Sectors targeted by law reforms or enforcement action

The Dutch Central Bank (the **DNB**) continues to pay close attention to supervised gatekeepers, including traditional and non-traditional financial institutions. Since 20 May 2020, providers have engaged in exchange services between virtual currencies and fiat currencies and custodial wallet providers must comply with the registration requirement under the AML Act. Acting in breach of the registration requirement is a criminal offence under the Economic Offences Act (**WED**).

Cross-border coordinated enforcement activity

The European Public Prosecutor's Office (the **EPPO**) became operational on 1 June 2021. The EPPO works with 22 participating Member States to investigate, prosecute and bring before a national court various types of criminal offences that affect the EU's financial interests. The EU body has already opened more than 300 cases, according to the chief prosecutor, Laura Kövesi. An investigation into millions of euros' worth of VAT fraud is currently being carried out in the Netherlands and other countries, including Germany, Bulgaria and Slovakia. Since the EU budget inevitably affects entities in the financial sector, it is expected that the EPPO will involve these entities in investigations in the near future.

The Netherlands is a member of the J5 Group, which consists of the tax enforcement authorities of the Netherlands, Australia, Canada, the UK and the US. These authorities share intelligence, gather information and conduct investigations in order to combat cross-border tax crime. In 2021, the focus of the J5 Group was on financial technology (**FINtech**) companies. FINtech companies often market new financial products and payment processes.

According to the Internal Revenue Service Criminal Investigation (the U.S. tax enforcement authority participating in the J5 Group), the FINtech industry is used by tax avoiders and money launderers. The J5 Group identified companies that will be subject to investigations by the participating authorities in the J5 Group, following leads suggesting criminal behaviour. Compliance with applicable tax and AML/CFT regulations should be and remain high on the agenda of compliance officers of FINtech companies.

Team High Tech Crime of the Dutch Police continues to play an important role in international cybercrime investigations. It regularly cooperates with authorities from other countries in international investigations into cybercrime, including large-scale abuse of the ICT infrastructure and ransomware attacks. Team High Tech Crime participated in 2021 in the disruption of Emotet. According to Europol, Emotet was more than just malware, as it was offered for hire to other cybercriminals to install other types of malware, such as banking Trojans or ransomwares, onto a victim's computer.

Financial crime issue predictions for 2022

The Dutch enforcement authorities remain focused on: (i) corruption; (ii) tax fraud; and (iii) cybercrime. We expect authorities to focus more on (iv) business human rights and environmental, social and corporate governance (**ESG**).

In line with the supervisory plans of the DNB for 2022, we expect to see a continued focus on (further) investigations into potential breaches of the AML Act by gatekeepers of the financial system. In view of the DNB, the efforts of financial institutions in the area of financial economic crime have increased, but not sufficiently. The DNB calls for better cooperation, both between public and private parties and at the European level.

Key team members

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

Fleur le Roy
Associate – Netherlands
Tel +31 682 359 843
fleur.leroy@allenovery.com

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

Sjoerd Lopik
Associate – Netherlands
Tel +31 20 674 1574
sjoerd.lopik@allenovery.com

Allen & Overy LLP's team is described as "offering expertise in both investigations and white-collar defence litigation" and "distinguished by its criminal defence capabilities"

Chambers Europe: White Collar Crime & Corporate Investigations 2021

Clients appreciate that Hendrik Jan Biemond "combines excellent legal expertise with diplomacy and convincing communication skills".

Chambers Europe: Dispute Resolution – White Collar Crime – 2021

South Africa

South Africa's white collar crime framework continues to develop in the wake of a series of "state capture" enquiries by the Special Investigating Unit (**SIU**) and National Prosecuting Authority (**NPA**). Together with former President Zuma's longstanding corruption trial relating to arms procurement in the late 1990s and activism on corporate accountability and environmental issues, this has led to clarifications regarding key issues in the investigation and prosecution of white collar crime. While South African courts have been particularly active in the past year, Parliament, National Treasury and regulators such as the South African Revenue Service (**SARS**) and Financial Intelligence Centre (**FIC**) have taken steps to consolidate and amend South Africa's regulatory framework to enhance corporate transparency and improve personal data and crypto asset regulation – developments likely to unfold in the next year. Major cross-border investigations to watch include the CumEx banking scandal while poaching continues to be a key focus of cross-border law-enforcement.

Investigations trends/developments

Contracting with the State

The first part of the report from the Judicial Commission of Enquiry into allegations of State Capture, Corruption and Fraud in the Public Sector including Organs of State, as chaired by Deputy Chief Justice Raymond Zondo (the Zondo Commission) has been handed to the President and was published online on 4 January. Some 874 pages in extent, the first part of the report contains numerous adverse findings by the Zondo Commission in regard to state capture and corrupt activity relating to South African Airways and associated entities, the South African Revenue Service (SARS) and irregular media procurement by Government and various State Owned Enterprises (SOEs) through the Gupta family, coupled with extensive referrals for further criminal investigation and prosecution by the National Prosecuting Authority (NPA) and steps to be taken for the recovery of misappropriated funds and forfeiture proceedings in relation to the proceeds of crime, where appropriate. Two further parts to the report are expected as at end January and February. The President in turn has undertaken to report to parliament by June on further action to be taken in implementing the findings and recommendations of the Zondo Commission.

The authorities continue to focus on investigating public sector corruption or "state capture". In the meantime, several "state capture" matters have been referred to the Special Investigating Unit (**SIU**), which has commenced investigation and civil recovery proceedings before the Special Tribunal while criminal prosecutions are being pursued by the National Prosecuting Agency (**NPA**). In parallel, there are indications that State-Owned Enterprises (**SOEs**) are moving towards administrative "self-review" before the High Courts in order to set aside contracts tainted by corruption and claim restitution of misappropriated funds. The consequent rapid development of public procurement and administrative law principles has important implications for private parties who contract with the State and will likely shape due diligence obligations when contracting with the government.

A new SIU focus is ZAR14.8 billion of misappropriated public funds associated with Covid-19 government tenders. While the most high-profile example is the "Digital Vibes" scandal, implicating South Africa's former Minister of Health, the SIU is reported to have sought ZAR1.39 billion in civil recoveries before the Special Tribunal, with 214 cases referred to the NPA for criminal investigation. The commencement of Special Tribunal sittings highlights its powers to order the preservation and forfeiture of private parties' assets and to set aside tainted contracts.

Significant law reforms impacting corporate criminal liability

Strengthening AML and CTF framework

The October 2021 publication of the Financial Action Task Force Mutual Evaluation Report on Eastern and Southern Africa (**FATF Report**) highlighted weaknesses in the proactive investigation of money laundering and terrorist financing, slow progress of prosecutions relating to terrorist financing, and difficulties obtaining information regarding the ultimate beneficial ownership records of companies and trusts.

The authorities have sought to remedy weaknesses in the corporate transparency regime (particularly in the disclosure of ultimate beneficial ownership) through the publication of the Companies Amendment Bill (**Companies Bill**) on 1 October 2021. Proposed amendments include obliging all companies (rather than only listed entities) to require shareholder disclosure of ultimate beneficial ownership; to publish details of persons who, alone or in aggregate, hold beneficial interests of 5% or more of shares of a particular class; and to lodge this information with the Companies and Intellectual Properties Commission. The proposed definition of a "true owner" mirrors that of the Financial Intelligence Centre Act (**FICA**) and aligns with the definitions provided by FATF. The Bill provides that these records be made available on request to shareholders and members of the public. If enacted, the Bill will require a greater degree of due diligence on the part of shareholders and also place an obligation on company secretaries and Boards to ensure that there are adequate procedures in place for responding to access to information requests. Liability for failure to take reasonable steps to do so within the shortened ten-business-day time period is an offence for which directors or prescribed companies may be held liable.

Public access to tax records

Taxpayer confidentiality is under review as a result of a November 2021 High Court judgment which declared provisions of the Tax Administration Act (**TAA**) and Promotion of Access to Information Act (**PAIA**) unconstitutional to the extent that the South African Revenue Service (**SARS**) may refuse public access to taxpayer records (and dissemination of such records by a requester), despite it being in the "public interest" to do so.

In this case, the "public interest" in accessing former President Zuma's tax returns was asserted by leading media outlets (based on allegations of tax avoidance by Mr Zuma during his presidency). The case follows a trend of social and media activism to hold public officials accountable for corruption and white-collar crime. SARS has confirmed its intention to oppose a confirmation of constitutional invalidity by the Constitutional Court and has sought leave to appeal the order. In the interim, taxpayer records are no longer immune to public scrutiny through access to information requests – albeit in exceptional circumstances.

New data protection regime

The Protection of Personal Information Act (**POPIA**), modelled on the EU General Data Protection Regulation (**GDPR**), is now fully in force. The new Information Regulator has commenced operations including assuming responsibility for enforcement. One of the first tests of how the Information Regulator is likely to interact with the police and NPA occurred in the past year in the form of a ransomware attack on the South African Department of Justice and Constitutional Development (**DoJ**) in September 2021. The resulting data breach included the Information Regulator's own data (which was being stored on the DoJ's IT systems).

Internal investigations – key developments

In-house legal and investigations teams should review internal compliance programmes and ensure that personal information is processed in accordance with POPIA. This includes:

– the appointment of an information officer

– compilation and assessment of any personal information already in possession

– adopting appropriate security measures to ensure the integrity and confidentiality of personal information

– verification of personal information

– ensuring that personal information is not retained for longer than is necessary to fulfil the purpose for which it was obtained

– deletion of unauthorised personal information.

In obtaining and processing personal information for an internal investigation, such information must be processed fairly and lawfully, with the consent of the data subject and for a specific purpose. Measures must be put in place to secure information obtained against loss, unlawful access, interference, modification, unauthorised destruction and disclosure.

Sectors targeted by law reforms or enforcement action

Crypto assets

A set of forward-looking law reforms to regulate crypto assets (in part to counter money laundering and terrororist financing) are gradually moving through the consultation process. The Intergovernmental Fintech Working Group (**IFWG**) published its position paper on crypto assets on 11 June 2021. The IFWG's 25 recommendations seek to draw Crypto Asset Service Providers (**CASPs**) into South Africa's broader regulatory framework, aimed at combatting money laundering and terrorist financing, regulating cross-border financial flows (implicating Exchange Control Regulations and the South African Reserve Bank's Financial Surveillance Department), and preventing fraud, consumer abuse and market misconduct.

The Financial Sector Conduct Authority (**FSCA**) published a draft declaration that crypto assets would be regarded as a "financial product" under the Financial Advisory and Intermediary Services Act, 37 of 2002 (FAIS) on 20 November 2020. The effect of the FSCA's declaration is to require that CASPs be authorised to advise or provide intermediary services (and applies to crypto asset exchanges and platforms, as well as brokers and advisors).

Electronic communications service providers

The Cybercrimes Act partly came into force on 1 December 2021, defining various types of cybercrime and obliging electronic communications service providers and financial institutions to provide assistance to police officers or investigators where required to do so. Provisions not yet in force include reporting obligations for electronic communications service providers and financial institutions in respect of certain types of cybercrimes.

This Act joins a small but growing body of laws in other jurisdictions, aimed at giving investigators direct access to data held by communication service providers. This sector, as well as the financial services sector, will need to be ready to respond.

Sectors with environmental impact

The evolving Karpowership controversy reflects the interplay of ESG considerations in the energy sector and the role of political, government and civil society stakeholders in matters under investigation by regulatory and prosecutorial authorities.

In a ZAR225 billion deal, the Turkish-led Karpowership consortium were selected as preferred bidders for South Africa's Risk Mitigation Independent Power Producer Procurement Programme. The national energy regulator has approved Karpowership's energy generation licence but the Department of Forestry, Fisheries and the Environment (**DFFE**) has rejected Karpowership's environmental impact assessment. Karpowership has appealed that decision. In the interim, the DFFE's enforcement unit (the "Green Scorpions") has recommended criminal charges against Karpowership's agents for intentionally misleading the DFFE and attempting to bypass environmental regulations. Separately, the Department of Mineral Resources and Energy is facing a legal review challenge by a disappointed bidder, seeking to overturn the tender award on the basis of allegations of corruption (which have been fiercely contested in the media and are subject to investigation by Parliament and SARS). The matter illustrates how a company can get caught up in the tensions between different government departments exacerbated by ESG considerations – here being the E (environment) and G (alleged corruption).

Cross-border coordinated enforcement activity

South Africa and the United Arab Emirates (**UAE**) concluded treaties on extradition and mutual legal assistance in 2018, which the UAE ratified in 2021. It is anticipated that these treaties will facilitate greater cooperation between South Africa and the UAE and assist in the investigation and prosecution of crimes. In particular, the treaty will assist the South African government in ensuring the return of the Gupta brothers, Atul and Rajesh, and their wives, Chetali and Arti, to stand trial for money laundering. The United Kingdom imposed sanctions on the Guptas in 2021 (already sanctioned under the U.S. "Magnitsky" regime in 2019). The Guptas wielded enormous political influence in South Africa and are heavily linked to state capture.

South Africa continues to cooperate both regionally and internationally in respect of anti-poaching operations, while also participating in the INTERPOL-supported Operation Afya II which concluded in July 2021. The operation, across Southern Africa, focused on investigating, intercepting and seizing counterfeit and illicit health products with an estimated value of USD3.5 million.

In July 2021, SARS and the United States Internal Revenue Service Criminal Investigation Division issued a statement announcing their cooperation. Their focus includes public corruption, cyber fraud and money laundering and, in particular, promoters, professional enablers and financial institutions. This partnership is part of a wider focus on cross-border illicit financial flows relating to poaching, mineral smuggling and the illicit tobacco and counterfeit textile trades. There is also a growing awareness of the links between environmental crime and money laundering.

Financial crime issue predictions for 2022

– **Strengthened financial crime response will likely see improved implementation of existing AML legislation and particular attention to corporate responsibility**: We expect to see a comprehensive response and follow-up actions taken in 2022 based on the recommendations in the FATF Report concerning South Africa's AML and CFT framework.

– **Pandora Papers disclosures**: The almost 12 million offshore financial asset records have not yet named South African individuals or corporations, however, reports indicate that there are some 56,493 links to South Africa and it is anticipated that further releases will name South African individuals or corporations. The likely consequence is coordinated investigation and possibly enforcement action commencing in 2022.

– **Dealing with the government**: The final report of the Zondo Commission will result in tightening measures to prevent government corruption, with a focus on SOEs. The fallout from the inquiry and the final report will continue to concern entities that conduct business with the South African government. As cases move through the prosecution and civil recovery processes, we anticipate further clarity regarding the applicable legal principles in relation to private parties contracting with the State.

– **Data privacy**: As the Information Regulator commences operations, in-house counsel will need to ensure internal and external investigations are carried out without breaching the new data privacy laws.

– **Corporate accountability**: Corporate accountability is likely to remain in the spotlight due to the activities of SARS while South Africa is seeing increasing awareness concerning the intersection between white-collar crime and environmental regulation. The environmental space is one to watch – particularly if the planned amendments to various environmental legislation are eventually enacted, as these not only aim to provide environmental investigators with greater powers, but also to expand the range of companies and individuals subject to the wide-ranging environmental duty of care.

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

Claire van Son
Candidate Attorney – Johannesburg
Tel + 27 10 597 9893
claire.vanson@allenovery.com

"They have some really good people. When international banks have regulatory or white-collar issues, they are one that they go to."

February 2021-February 2022, Chambers Global Guide – Global-wide: Corporate Investigations

"Distinguished investigations practice with extensive experience dealing with enforcement agencies around the globe."

February 2021-February 2022, Chambers Global Guide – Global-wide: Corporate Investigations

"Prominence in business rescue and insolvency cases, financial services disputes, construction, and compliance and investigations."

April 2021-April 2022, Legal 500 – South Africa: Dispute Resolution

"The service was world-class. The client and I were extremely satisfied; results exceeded our expectations."

February 2021-February 2022, Chambers Global Guide – Global-wide: Corporate Investigations

United Arab Emirates

2021 has seen the UAE implement a raft of measures to enhance its AML and CTF capabilities, including making key amendments to AML legislation, the issuance of new joint agency guidance on AML and CTF compliance, and the establishment of a new federal AML/CTF agency and a money laundering specialist court in Dubai. These actions have implications for both the UAE's onshore jurisdiction and its key offshore jurisdictions including the Dubai International Financial Centre (the **DIFC**) and the Abu Dhabi Global Market (the **ADGM**). These developments place a key focus on expanding the scope of the UAE's AML/CTF regime and increasing the monitoring of high-risk sectors for financial crime (including emerging areas of the financial services industry such as virtual assets).

There have also been developments which have aimed to enhance the UAE's anti-bribery and corruption compliance credentials, make whistleblowing protections clearer and make corruption and compliance reporting easier.

The pace of regulatory change and development (in particular in the area of combatting financial crime) is likely to continue, and so it remains of crucial importance for businesses to have robust systems and controls in place to understand, adapt to and ensure ongoing compliance with the quickly changing and increasingly complex regulatory environment in the UAE.

Significant law reforms

The Financial Action Task Force's (**FATF**) April 2020 Mutual Evaluation Report (**MER**) on the UAE identified a number of areas where the UAE's framework for combatting financial crime required significant improvement. In 2021 the UAE consequently took actions to embed and enhance the practical effectiveness of the UAE's AML/CTF regime.

Expanded AML Laws

Amendments made by the Amendments to Federal Decree 20 of 2018 (**the AML Law**) significantly expand the scope and application of the AML Law. They:

- broaden the definition of "funds" (which can be deemed as proceeds of crime) to include economic resources of any type including natural resources (such as oil and gas), bank credits, cheques, payment orders, shares, bonds, securities, bills and letters of credit and virtual assets of any kind; and
- introduce definitions of "virtual assets" and "virtual assets service providers" (**VASPs**), and bring certain virtual assets and VASPs within the scope of the AML Law. VASPs must now comply with AML/CTF compliance measures, such as customer due diligence and suspicious activity reporting.

The amendments make it easier for enforcement authorities to combat money laundering and terrorist financing activity in respect of a broader range of criminal property.

New AML and CTF guidelines for businesses

New joint AML/CTF guidelines were issued by the UAE Central Bank, the Dubai Financial Services Authority (the **DFSA**) and the ADGM's Financial Services Regulatory Authority (the **FSRA**) (the **Guidelines**) in June 2021.

The Guidelines more clearly explain AML/CTF regulatory obligations and expectations for Financial Institutions and Designated Non-Financial Businesses and Professions (**DNFBPs**) (such as real estate professionals, precious metal dealers and legal services providers) which fall within the scope of the UAE's AML/CTF regime. The Guidelines state what authorities consider to be good and bad practice in respect of key aspects of AML/CTF compliance such as governance and culture, policies and procedures, customer due diligence and suspicious activity reporting.

The UAE Central Bank issued the "Anti-Money Laundering and Combatting the Financing of Illegal Organisations Guidelines for Financial Institutions" (the **CB Guidelines**). The CB Guidelines provide detailed guidance on the measures that financial institutions are required to implement in order to comply with legal and regulatory requirements. The CB Guidelines highlight that a risk-based approach is central to the effective implementation of applicable AML/CTF legislation and that a key requirement for taking an effective risk-based approach is that a financial institution properly understands the money laundering and terrorist financing risks to which it is exposed.

New AML/CTF guidance for licensed exchange houses (the **LEH Guidelines**) was issued in November. The LEH sector is considered a priority due to its exposure to cash and cross-border transactions. The LEH Guidelines require licensed exchange houses to conduct a regular risk assessment that covers all commensurate risks to their exchange business.

New regulatory frameworks for virtual assets

In 2019, the ADGM was the first jurisdiction in the world to introduce a bespoke framework to regulate virtual assets. In 2021, the UAE took further steps, which have implications for its AML/CTF regime.

- In September 2021, the UAE National Committee for Combatting Money Laundering and Financing of Terrorism and Illegal Organisations (**NAMLCFTC**) announced the adoption of a regulatory framework for virtual assets in the UAE. The UAE Central Bank and the Securities and Commodities Authority will oversee its implementation. The framework is a first step in providing comprehensive regulation of virtual assets and will improve safeguards in the financial system to protect investors from money laundering and terrorist financing risks.
- In October 2021, the DFSA launched a new regulatory framework for investment tokens issued or traded within the DIFC. This framework will bring VASPs who provide investment tokens within the scope of the DFSA licensing regime and make them subject to the AML/CTF requirements which apply to DFSA-authorised firms. Our expectation is that, in 2022, the DFSA will expand its regulatory perimeter to include a wider range of virtual assets.

New specialist money laundering court in Dubai

It is perhaps no surprise, given all these developments, that the Dubai Courts have announced a new specialist court for money laundering and tax evasion crimes. It will be staffed with judges with specialist money laundering experience.

New anti-bribery and corruption rules

2021 has seen further developments aimed at enhancing the UAE's anti-bribery and corruption compliance credentials.

The Abu Dhabi Accountability Authority (**ADAA**) is the independent Abu Dhabi government authority responsible for promoting the principles of accountability, transparency and integrity across the Abu Dhabi government. The ADAA has power of oversight over all Abu Dhabi government departments and agencies and corporate entities which are wholly or partially owned by the Abu Dhabi state.

In March 2021, the ADAA issued new Anti-Corruption Regulations which create powers for the ADAA to investigate bribery and corruption, introduce new reporting procedures and provide whistleblower protections for employees of government agencies and entities subject to the ADAA's oversight.

Whistleblowing regime developments

The UAE has taken further steps to develop and embed protections for whistleblowers in both its onshore and offshore jurisdictions and to make whistleblower reporting easier, following the introduction of a federal whistleblowing protection law in 2020.

UAE Central Bank whistleblowing portal

In June 2021 the UAE Central Bank set up a whistleblowing portal on its public website to allow Central Bank employees and third parties to report any corruption, fraud, undisclosed conflicts of interest, ethical violations or non-compliance with applicable laws and regulations by Central Bank employees, contractors or representatives. As the UAE's whistleblowing regime becomes more sophisticated, we expect businesses will come under increased pressure to put in place practical measures to ensure misconduct can be effectively, safely and anonymously reported.

Proposed new whistleblowing rules for certain entities

On 7 July 2021, the DFSA issued a consultation paper seeking public comment on proposals to introduce whistleblowing measures for DFSA-authorised firms, DNFBPs and other regulated entities operating within the DIFC. The proposed whistleblowing measures introduce various requirements and protections which build on existing requirements and aim to move towards a more consistent approach to reporting and recording misconduct.

The consultation closed on 7 September 2021. Consequential amendments to the DIFC Regulatory Law and the DFSA's Rulebook and Sourcebook are expected in 2022.

Investigations – key developments/trends

The UAE Cabinet approved the establishment of the UAE Executive Office of Anti-Money Laundering and Countering the Financing of Terrorism (the **EO**) in February 2021. The EO reports directly to the Higher Committee overseeing the UAE's national AML/CTF strategy and is chaired by the UAE's Minister of Foreign Affairs and International Cooperation. The EO's responsibilities include actively increasing information sharing between law enforcement agencies, supervisors, and the private sector. We can expect to see this resulting in increased enforcement.

In November 2021, the UAE announced its first ever comprehensive federal data protection law. This means that UAE businesses will need to significantly adapt how they interact with personal data. The new law will have significant implications for how businesses conduct investigations and report information to government authorities. For more detail, see this article on the new UAE data protection law.

Cross-border coordinated enforcement activity

Cross-border cooperation has increased significantly.

Perhaps the most widely reported development in this area was the signing of a peace treaty between the UAE and the State of Israel on 15 September 2020, as part of the Abraham Accords. The peace treaty provides for the normalisation of relations between the two countries and specifically contemplates the execution of further bilateral agreements aimed at increasing cooperation on a raft of issues such as legal matters and information sharing. We expect to see further cooperation in 2022 as the peace treaty takes full effect.

The UAE and the UK Governments entered into a new partnership to tackle illicit finance. The partnership will bolster law enforcement by enhancing intelligence sharing and joint operations between the UK and UAE against serious and organised crime networks.

The DFSA is continuing to work closely with its counterparts across the globe. In addition to the 108 bilateral and six multilateral memoranda of understanding the DFSA has signed with other regulators, there are ongoing discussions with Brunei, India, Israel and Italy to put similar arrangements in place. During the past year, the DFSA received 81 regulatory requests for information and assistance from other regulators, while the DFSA made 109 requests to fellow regulators for information.

The EO will also play a key role in promoting the coordination of cross-border enforcement activity and information sharing. The EO's responsibilities include improving national and international coordination and cooperation on AML/CTF issues at the policy and operational levels. The EO will also tackle money laundering and terrorist financing threats by working with regional and international groups, such as the FATF.

Sector focus

Virtual assets

There has been a flurry of activity in 2021 to expand the UAE's AML/CTF regulatory regime to cover certain types of virtual assets and virtual asset services providers (**VASPs**) to bring the UAE closer in line with the FATF's 2018 and 2019 recommendations regarding virtual assets regulation and to promote the UAE as an attractive market for virtual asset trading (see above).

Predictions for 2022

Compliance monitoring and enforcement activity will increase as the UAE's AML/CTF regime matures

Monitoring practical AML/CTF compliance by businesses will become a higher priority for UAE enforcement authorities as the AML/CTF regime expands and matures. We expect to see higher levels of financial crime-related enforcement activity in 2022 and more significant penalties where non-compliance is identified.

Businesses (and their in-house legal teams) should focus on being able to demonstrate effective compliance with both strict AML/CTF legal requirements and the more detailed AML/CTF practical guidance issued by the UAE authorities this year (see above on the Guidelines, the CB Guidelines and the LEH Guidelines).

Virtual assets

We expect to see further steps taken in 2022 to broaden both the onshore and offshore AML/CTF regulatory regimes to capture a wider range of virtual assets and the businesses that provide them. Accordingly, VASPs should keep a close eye on regulatory developments in respect of virtual assets to ensure that they do not inadvertently fall afoul of regulatory requirements which do not currently apply to them but which may apply to them from 2022.

Whistleblowing

We also expect to see the UAE take steps to further enhance and embed whistleblower protections. As expectations around, and monitoring of, whistleblowing cases and procedures increase, businesses will need to ensure that they have adequate procedures in place to enable their employees and other stakeholders to effectively, safely and anonymously report misconduct.

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

"Yacine Francis frequently represents banks and other financial institutions, often adeptly advising on corporate investigations within the financial services sector. Peers comment: 'He is technically excellent, client-friendly and very well thought of.'"

Chambers Global 2021 – UAE (Dispute Resolution)

"Particularly respected for its presence in the DIFC Courts, notably in financial services and white-collar crime cases."

Chambers Global 2021 – UAE (Dispute Resolution)

"In addition to its experience handling financial services and securities disputes, the team is further noted for its strong track record in construction matters and corporate investigations."

Chambers Global 2021 – Middle East (Dispute Resolution)

United Kingdom

Money laundering was firmly in the sights of the UK authorities in 2021 and will remain so in 2022. The Financial Conduct Authority (**FCA**) brought is first prosecution against a bank under the UK Money Laundering Regulations, and the UK's entire CTF/AML regime is currently under review. The AML supervision of crypto assets will likely evolve in 2022 as it is considered a high-risk area.

New criminal offences relating to defined benefit pension schemes were introduced but the consultation on corporate criminal liability more generally is still ongoing, with a report expected from the Law Commission shortly. Big Tech companies are under pressure to reduce online harms, with new criminal offences possibly being introduced in 2022 via the Online Safety Bill.

The Serious Fraud Office (**SFO**) is likely to be focusing on frauds on the public purse committed during the pandemic. It will also be trying to regain its enforcement momentum after some difficult (for the SFO) court decisions which curtailed its ability to obtain documents held abroad and raised criticisms of the SFO's lack of disclosure in some high-profile cases. 2021 saw the number of new SFO corporate criminal investigations fall to the lowest number (four) in over a decade.

Internal investigations into ESG-related issues are becoming much more common, as investors and employees seek to exert pressure on companies to improve treatment of their workers in supply chains and lessen environmental impact.

Investigations trends/developments

Access to documents held overseas

The Supreme Court ruled that the SFO does not have the power to order the disclosure of documents held abroad by a non-UK company: KBR Inc v The Director of the Serious Fraud Office [2021] UKSC 2. The decision dealt a blow to the UK's Serious Fraud Office (**SFO**) with the unanimous rejection by the court of the SFO's attempted expansion of its statutory powers to compel documents from foreign parent companies. The decision will have ramifications for other UK authorities seeking to compel production of material from non-UK parent companies without any domestic presence. The SFO will instead need to rely on Mutual Legal Assistance regimes which can be cumbersome. The SFO has not yet been able to take advantage of the Crime (Overseas Production Orders) Act 2021 to access data directly from overseas communication service providers despite a bilateral agreement having already been signed between the UK and U.S.

UK-based companies should note that documents in their possession or control, but held overseas, may fall in scope of the SFO's document disclosure powers and, subject to contrary statutory intent, production powers of other authorities too. This construction of the SFO's powers was not challenged by the parties in the KBR case and therefore not decided by the Supreme Court, although the commentary did appear to favour this view.

M&A: Innocent acquirers and deferred prosecution agreements

The SFO entered into a deferred prosecution agreement (**DPA**) with Amec Foster Wheeler Energy Limited (formerly Foster Wheeler Energy Limited) (**company**) and the John Wood Group plc (**Wood**) to settle historic bribery claims. Wood purchased the company in 2017, just after the SFO commenced its investigation.

This DPA involved an innocent parent company (Wood) which purchased a subsidiary (the company) after the misconduct (bribery by the subsidiary) had already occurred. As part of considering whether to approve the DPA, the judge wanted to know whether the acquisition price of the subsidiary had been reduced to reflect the risk of penalty (it had not been). The judge was reassured that the offer price was based on publicly available information, and that the SFO investigation was not factored into the valuation because it was announced after the offer was made. If the purchase price had been reduced, it is likely that the court might have viewed the appropriateness of the proposed penalty (which had been reduced to reflect the fact that this was historic conduct) in the DPA differently.

This DPA joins two others examples involving companies that had been taken over by innocent acquirers where all, or the vast majority, of the misconduct in question occurred prior to the change in ownership and certainly without the knowledge of the acquirer.[3] In both, on discovery of the misconduct (post-acquisition) there was self-reporting and cooperation with the SFO. In the Amec Foster Wheeler case, the buyer was aware of the SFO investigation, albeit after a price had been agreed. These three DPAs together show three buyers of companies with historic bribery issues who chose to cooperate with the SFO, and earnt a discounted penalty as a result.

Treatment of individuals

The SFO has continued to fail to secure convictions of individuals following DPAs, most recently due to disclosure failings by the SFO. Concerns about the impact of DPAs on inculpated individuals were moderately ameliorated by greater protection afforded by the court during the approval of a DPA with Amec Foster Wheeler. For the first time, the court ordered that DPA-linked documents must have a warning that there is no finding of fact concerning the culpability of any individual. The DPA was also not published.

Cooperating offenders

The recent sentencing of an oil services company[4] for a failure to prevent bribery is an example of the SFO using a cooperating offender (a former Global Head of Sales) to help secure a conviction against a company. The individual, as a result of his cooperation, managed to avoid prison (he received a suspended sentence) despite being convicted of multiple counts of bribery. The SFO is keen to "flip" more offenders like this, but the risk/benefit analysis for the individual is not straightforward as they must provide a lot of incriminating information without any guarantee of being treated more leniently and at a time when it is not certain that they would be charged with any offences, absent cooperation.

Fewer big bribery cases – more domestic fraud enforcement?

The SFO appears to be focusing on smaller, domestic cases that can be progressed more quickly. It has only publicly announced one cross-border bribery investigation in the past year: the probe into a Canadian aircraft maker's conduct in Indonesia.

The pandemic created a perfect environment for fraud including, for example, push-payment fraud on individuals and businesses. It remains to be seen how effective the UK authorities will be at taking action against the huge amount of fraud which took place during the pandemic.

Money laundering as a continuing focus for the authorities

In the UK, money laundering has remained a focus for regulators in the financial services and other sectors, including the art sector which is likely to come under greater scrutiny after HMRC published its first risk assessment on art market participants in June 2021. The art market, alongside trust or company service providers, is considered as representing the highest inherent risk for money laundering.

The UK Gambling Commission has been active in imposing fines for AML breaches. HMRC has also taken enforcement action and in January 2021 imposed a GBP23.8 million fine on a money service business for breaches[5] of the Money Laundering Regulations 2017.

Two of the biggest sanctions imposed by the FCA in the 12 months prior to March 2021 related to failures to address financial crime and AML risks. Both cases highlighted inadequate systems and controls "where one could be forgiven for thinking the true function and meaning of the controls had become lost in elaborate processes leading to failure".

The FCA is keen for firms to focus on the harm that regulations are seeking to prevent as opposed to treating regulations as an end in themselves. The FCA achieved its first successful criminal conviction of a bank for breaches of the Money Laundering Regulations, and we can expect to see the FCA pursuing more dual-track investigations.

Compliance programmes

Building on the guidance on how to evaluate a compliance program that it released in 2020, the SFO has pledged to deepen its understanding of compliance and engagement with compliance professionals. The director of the SFO, who comes with compliance expertise from a previous role, said: "we're upskilling ourselves to be better and smarter in this evaluation, including bringing in people with experience and expertise in this area".[6] Any enforcement action by the SFO is likely to therefore involve more in-depth scrutiny of compliance programmes. We have drawn together some common weaknesses in corporate compliance programmes.

Follow-on group actions

Group action by investors against companies[7] off the back of enforcement action remains a reality, although it is too early to tell whether these types of claims will gain much traction. Companies need to assess the risk of this happening early as it may impact decisions made on self-reporting, privilege and cooperation during the enforcement stage.

3_ICBC Standard Bank and Guralp
4_Petroface
5_MT Global
6_Society of Corporate Ethic interview (February 2021)
7_Allianz Global Investors GmbH and others v. G4S PLC; Manning & Napier Fund, Inc & Anor v Tesco plc.; Allianz Global Investors GmbH v RSA Insurance Group Ltd (formerly RSA Insurance Group Plc); Trustees for the Victory Portfolios & oths v Standard Chartered Bank

Significant law reforms impacting corporate criminal liability

There have been several legislative developments in a number of white-collar crime areas.

High-profile collapses of some large companies, and the resulting impact on their pension schemes, has led to two new criminal offences under the Pensions Schemes Act 2021, which came into force on 1 October 2021. They are aimed at improper conduct in relation to defined benefit pension schemes: (1) avoidance of employer debt; and (2) conduct risking accrued scheme benefits. As discussed previously, the new offences caused a stir in the pensions industry and beyond due to the broad scope of potential criminal liability (which could include any person involved with a defined benefit pension scheme, however tangentially) and the limited nature of the possible defences. The penalties are significant, including an unlimited fine and/or up to seven years' imprisonment, or a civil penalty of up to GBP1 million.

The UK Government introduced a new global corruption sanctions regime in April 2021. A Minister can designate individuals and companies who are suspected of involvement in corruption. There have already been sanctions made against individuals involved in corruption cases in Russia, South Africa, South Sudan and Latin America. These new sanctions will inevitably add to the complexity and compliance-related risks for businesses transacting and investing in higher-risk jurisdictions.

The UK Government is also consulting on an overhaul of the UK's AML/CTF regime. Despite no longer being an EU Member State, the UK will likely want to remain compliant with the FATF regime. The consultation is looking at overall effectiveness, sectors in scope, and whether supervisors have adequate powers to ensure compliance. Specific regulatory aspects being scrutinised are the risk-based approach, whether the MLRs enable the safe and effective use of technology to tackle AML/CTF, and improving the quality of suspicious activity reports. There is a separate consultation on amendments to the MLRs in particular, looking inter alia at supervisor access to SARS, proliferation financing, making reporting on beneficial ownership discrepancy reporting an ongoing obligation (not just at outset of relationship) and transfers of crypto assets.

Efforts to reform English law on corporate criminal liability continue to rumble on, with the Law Commission consulting on corporate criminal liability. Supporters of reform point to recent failures of the SFO to prosecute large corporations and senior individuals as evidence of the need for reform. One of the options under consideration is extending the "failure to prevent" model of corporate criminal liability, which is employed for bribery and tax evasion, to cover other types of economic crime.

The UK's current legal framework on debarment was adopted from EU law, and is currently being amended. Under existing legislation, debarment can be mandatory or discretionary, depending on the misconduct. The results of a UK government consultation were published on 6 December 2021. It sets out new mandatory and discretionary grounds for exclusion. Whilst further details are awaited, it looks like offences requiring mandatory debarment will be broadened to include fraud and fraudulent trading, theft, modern slavery offences, corporate manslaughter or corporate homicide, tax evasion, and the 'most serious' competition law breaches. The Government estimates that the new legislation will come into force in 2023.

Internal investigations – key considerations

A forensic report produced by PWC for a corporate client's internal investigation was ruled not to be privileged in *State of Qatar v Banque Havilland SA & Ors* [2021] EWHC 2172 (Comm) (30 July 2021) LP because the report was not produced for the sole or dominant purpose of contemplated litigation. The case is a reminder of how tricky it can be to invoke litigation privilege to protect third-party communications in the context of early stage investigations.

Sectors targeted by law reforms or enforcement action

Enforcement action has been taken across a range of sectors in 2021. However, updates to the UK Government's economic crime plan 2019-2022 refer in particular to the following areas of focus:

– AML supervision of crypto assets

– AML and professional "enablers" (accountancy, law, company service providers)

– bribery and corruption in the oil and gas, extractive and overseas development sectors

– fraud against the public sector.

The May 2021 Statement of Progress identifies a "strong focus on fraud", money laundering, seizing more criminal assets, and strengthening corporate transparency.

AML is prominent here, and aligns with the UK's review of its entire AML/CTF legal framework (see above). This means that those businesses that fall within the scope of the UK Money Laundering Regulations 2017 (and those that may do so as a result of reforms) will be under the spotlight of the authorities. These businesses are very much regarded as part of the public-private partnership response to combatting economic crime.

Fines for failure to prevent financial crime remain among the highest levied by the FCA and Prudential Regulation Authority regulators (with four fines totalling GBP421 million between October 2020 and October 2021). The Financial Conduct Authority is demonstrating a bolder risk appetite and willingness to use its criminal prosecution powers in financial crime cases.

We also expect to see increased scrutiny of businesses which sell themselves as aiding sustainability, not just from activist investors. For example, the SFO is prosecuting two former directors of an ethical forestry investment plan which promoted a project to put money into tree plantations in the Brazilian rainforest.

The Online Safety Bill is currently being considered into Parliament, and is likely to come into force in 2022. A new duty of care will apply to search engines and providers of internet services which allow individuals to upload and share user-generated content. The Bill is aimed at Big Tech and will rely initially on enforcement by regulatory fines (Ofcom will have the power to issue fines of GDP18 million or 10% of the entity's worldwide revenues, whichever is higher). However, if the regime is not effective at making Big Tech firms reduce online harm, the Bill provides for new criminal offences aimed at senior executives of Big Tech firms to be introduced where they have failed to take reasonable steps to prevent offences being committed. At present this would happen after two years, although the UK Culture Secretary said in November 2021 that she wants to accelerate the timing of this new criminal regime to between three and six months.

What examples do you have of cross-border coordinated investigation or enforcement activity in your jurisdiction in 2021?

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 she attaches to international cooperation. Both the SFO and the FCA have secondees from overseas enforcement authorities.

There is no such thing as a global settlement, but we have seen coordinated settlements, for example:

– In 2021 a crediting agreement was entered into by the SFO, the Department of Justice (DoJ), and the Securities and Exchange Commission (SEC) with respect to bribery by Amec Foster Wheeler in Brazil. The agreement operates by offsetting sums paid by the company to the SFO against the amounts due from Amec Foster Wheeler entities to the DoJ and the SEC. The Brazilian Authorities are also party to an agreement with the U.S. authorities which relates to the sum due from the company as a result of the offending in Brazil.

– Since October 2020, the FCA has imposed two significant penalties for failure to prevent financial crime that formed part of a "globally coordinated resolution". In both cases, the financial penalty imposed by the FCA took into account settlements reached with authorities in overseas jurisdictions.

The UK-EU Trade and Cooperation Agreement, implemented in the UK by the EU (Future Relationship) Act 2020, contains provisions on cooperation in criminal matters, including for mutual legal assistance and the freezing and confiscation of criminal property. It is too early to tell how this new regime will operate, but it is unlikely to be as timely or effective for law enforcement authorities as the EU-wide mechanisms in place pre-Brexit. Informal cooperation is likely to continue, but for now we may see the UK's investigation of serious crime involving Member States taking longer.

What are your predictions for the sorts of white-collar crime or investigations issues that will be troubling in-house legal and investigation teams/GCs in 2022?

– 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.

– Crime rises when individuals are under financial pressure. Post Covid-19, the combination of remote working, reduced compliance budgets, volatile markets, stressed supply chains and financial pressure may lead to an increased risk of financial crimes such as market abuse, fraud and misleading the market. GCs 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 may see businesses seek to penetrate new markets, clients and industry sectors in 2022. This may bring a higher corruption risk.

– 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.

– A careful trade-off is required when considering whether to self-report. GCs will need to be well-informed of any legal obligations to report (eg in regulated sectors). Outside regulated sectors GCs should consider current enforcement priorities and the pros and cons of reporting/cooperating. GCs will need to consider, as part of this analysis, the likelihood of follow-on claims (eg by investors) or connected investigations in other jurisdictions.

– Data protection questions will inevitably remain a hot topic for all during cross-border investigations. In the GIR guide to Data Privacy & Transfer in Investigations 2021/2 experts from Allen & Overy help those involved in investigations adopt a risk-based approach to the rules across 15 jurisdictions, thus ensuring investigations run smoothly

– 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

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

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

"…stands out for its ability to handle both civil and criminal issues arising in domestic and cross-border investigations into money laundering, corruption and sanctions violations."

Legal 500 UK – Regulatory Investigations and Corporate Crime 2021

"Exceptionally high levels of knowledge of the current state of anti-bribery and corruption regulation, legislation and enforcement in the UK and US, combined with a high level of understanding of the UK criminal justice system."

Legal 500 UK – Fraud: White-Collar Crime 2021

"Highly reputed across compliance and regulatory investigations, including anti-bribery matters."

Chambers UK – Financial Crime: Corporates 2022

"It's an extremely professional team – they're always available, responsive and give pragmatic but robust advice."

Chambers UK – Financial Services: Contentious Regulatory 2022

U.S.

The Biden Administration, including the President himself, has signaled an intent to aggressively ratchet up enforcement efforts on many fronts, spanning both the criminal and civil contexts. The US Department of Justice (**DOJ**), Securities and Exchange Commission (**SEC**), Commodity Futures Trading Commission (**CFTC**), and Federal Trade Commission (**FTC**), among other regulatory agencies, have all shown signs of a more zealous enforcement approach, which marks a change in the regulatory landscape compared to that of the prior administration. The shift toward an aggressive regulatory environment includes the deployment of more proactive investigative methods, a greater focus on prior misconduct, increasingly stringent corporate resolutions, and broader theories of corporate liability. These changes have undeniable implications for companies in all sectors, such as: (1) the need for robust compliance programs that incorporate strong prophylactic controls and remediate misconduct appropriately; and (2) the increasing importance of expert legal advice in navigating the heightened expectations of regulators and understanding the regulatory risks companies face in conducting their operations.

DOJ corporate criminal enforcement

The Biden Administration has been persistently vocal in announcing more rigorous enforcement priorities to thwart corporate criminal conduct. Top officials from the DOJ have announced a broad policy agenda that will "invigorate" the agency's efforts to confront corporate criminal misconduct.

The most impactful of these officials' statements came from Deputy Attorney General Lisa Monaco in October 2021.[8] Monaco announced that:

- To be eligible for any cooperation credit, a company must identify all individuals involved in the misconduct, regardless of their position, status, seniority, or level of involvement in the misconduct. Cooperating companies will be required to provide all non-privileged materials related to the identified individuals. This directive marks a slight escalation from the DOJ's prior policy of allowing cooperating companies to disclose only the individuals whom the companies determine to be "substantially involved" in the criminal conduct.
- The DOJ will evaluate "all prior misconduct . . . when it comes to decisions about the proper resolution with a company, whether or not that misconduct is similar to the conduct at issue in a particular investigation." As such, federal prosecutors are now directed to comprehensively assess a company's entire criminal, civil, and regulatory record in making charging decisions.
- Prior guidance from the DOJ that "suggested that monitorships are disfavored or are the exception" is rescinded. Thus, to the extent one existed, there is no longer a presumption against the imposition of a corporate compliance monitor.

Deterring misconduct by repeat corporate offenders

Perhaps the most notable policy announced by Deputy Attorney General Monaco is the DOJ's consideration of whether repeat corporate offenders — companies that have reached previous resolutions with the DOJ, regardless of office or section — should be granted a non-prosecution agreement (**NPA**) or deferred prosecution agreement (**DPA**). Monaco indicated that the DOJ will consider whether the opportunity to receive multiple NPAs and DPAs "instills a sense among corporations that these resolutions and the attendant fines are just the cost of doing business". The DOJ will consider whether there are other approaches that will have a greater impact on deterring misconduct.

Depending on the conclusion the DOJ reaches, DPAs and NPAs may, going forward, be unavailable to certain companies with a history of recidivism. Monaco made clear that "there will be serious consequences for violating [the] terms" of DPAs and NPAs, and the DOJ will be studying whether companies under an NPA or DPA "take those obligations seriously enough". As evidence of the DOJ's position, Monaco noted that two multinational corporations recently received a breach notification from the DOJ.

Proactive detection of foreign corruption

The growing link between issues of national security and corporate criminal misconduct is likely to yield greater enforcement. Monaco recognized that "[c]orporate crime has an increasing national security dimension." In June 2021 President Biden declared that the fight against global corruption is a core national security interest and directed his administration to better fight corruption through enforcement and cooperation with regulators around the world.

The Administration's prioritization of combatting global corruption as a national security concern has considerable implications for the enforcement of the Foreign Corrupt Practices Act (**FCPA**), which is the country's chief legal mechanism for rooting out and punishing corruption abroad. Indeed, top officials at the DOJ have signalled a changing approach to FCPA enforcement. FCPA investigations are increasingly conducted via proactive means (e.g., through proactive data mining for investigative leads, use of law enforcement sources and cooperators, and active cooperation with foreign governments) and rely less on companies self-reporting FCPA violations.[9]

The Biden Administration's emphasis on combatting global corruption along with the DOJ's increasing deployment of proactive investigative methods are, taken together, likely to yield an aggressive FCPA enforcement environment for the foreseeable future. An aggressive enforcement approach to the FCPA, however, is simply one example of the broader shift in corporate criminal enforcement that Deputy Attorney General Monaco announced. As she indicated in her closing remarks, Deputy Attorney General Monaco's statements mark the beginning, not the end, of actions the DOJ will take in its renewed emphasis on corporate criminal enforcement.

8_October 28, 2021 keynote speech at the American Bar Association's 36th National Institute on White-Collar Crime.

9_Then-Acting Assistant Attorney General Nicholas McQuaid at the June 2021 ACI FCPA Conference, and then-Acting Fraud Section Chief Daniel Kahn: "We have upped our detection, and we are learning of cases through a number of different ways."

Increasing DOJ resources and toolkit

The DOJ is "building up to surge resources for corporate enforcement" and has "started to redouble [its] commitment to white-collar enforcement."[10] The DOJ uses sophisticated data analytics to investigate suspected white-collar crime. The Fraud Section has, for a long time, used such analysis in financial services and healthcare fraud, as well as the use of data analysis in connection with insider trading cases by the SEC and the U.S. Attorney's Office for the Southern District of New York.

Areas of focus: sanctions, export controls, cryptocurrency

Sanctions and export control and cryptocurrency are likely to be specific areas of focus.

There has been a recent and significant increase in sanctions and export control investigations. There are approximately 150 current sanctions and export control investigations. The DOJ is likely to use new tools in export and sanctions cases, including a more rigorous use of asset forfeiture mechanisms.

Regarding cryptocurrency, Principal Associate Deputy Attorney General Carlin has said the area is "ripe for innovation and vigorous enforcement" and that the Bank Secrecy Act will be a critical component of the DOJ's efforts in that regard.

Like the FCPA, sanctions and export control and cryptocurrency enforcement are likely only the tip of the iceberg in terms of the DOJ's plans for greater corporate criminal enforcement. Given the challenging enforcement environment ahead, companies must heed Deputy Attorney General Monaco's warning that "[c]ompanies need to actively review their compliance programs to ensure they adequately monitor for and remediate misconduct — or else it's going to cost them down the line."

10_John Carlin, the Principal Associate Deputy Attorney General. Remarks made on October 5, 2021 during a Global Investigations Review panel.

SEC

The SEC, so far in the Biden Administration, has also signaled an aggressive enforcement tone. At the Securities Enforcement Forum program on November 4, 2021, SEC Chairman Gary Gensler was strident in his rhetoric: "[t]he Commission will make war without quarter on any who sell securities by fraud or misrepresentation" (quoting a 1934 speech from Joseph P. Kennedy, the first SEC Chairman) and "[t]hat means holding individuals and companies accountable, without fear or favor, across the approximately USD100 trillion capital markets we oversee."

Gensler stressed that cooperation means more than meeting legal obligations and "self-serving, independent investigations." In order to receive cooperation credit, a person or organization must provide genuine helpful cooperation that advances the SEC's case, not simply provide documents and testimony as required by law.

Echoing Monaco's remarks on repeat offenders, Gensler stated that the organization's entire history is relevant when assessing penalties. He also questioned whether NPAs and DPAs are appropriate for recidivists. This is a position that will be of concern to securities firms and other regulated entities that fall foul of the SEC's rules from time to time despite the best of intentions and world-class compliance programs.

Making an example

Of note from Gensler's speech was his focus on "high-impact" cases. Gensler stated:

"A high-impact case pulls many other actors back from the line. This prompts legal alerts, client letters and bulletins to go out. Compliance departments, lawyers and accountants change internal procedures as well. Such high-impact cases are important. They change behavior. They send a message to the rest of the market, to participants of various sizes, that certain misconduct will not be permitted. Some market participants may call this "regulation by enforcement." I just call it "enforcement.""

What does this mean? Likely, it means a focus on cases in areas that Gensler has identified, such as Crypto, Cybersecurity, ESG, SPACs, retail investor conflicts, and the FCPA. In those areas we can expect the SEC to seek significant relief, including outsized penalties to drive home the SEC's positions.

Reducing timelines

The SEC Chairman and other SEC officials at the Securities Enforcement Forum program also referenced a number of procedural shifts to speed up SEC investigations. Gensler noted that the defense bar often makes a strategic decision to burn the clock and, in response, he has directed the staff to cut back on meetings, especially during the Wells process. SEC Enforcement Director Gurbir Grewal indicated that he is instilling a sense of urgency in his staff to quickly complete investigations, and that he trusts the staff to get it right so that appeals of the staff's judgment or views should be limited and quite targeted.

Higher penalties

Finally, SEC officials have talked about the limited relevance of the precedent of prior SEC actions in determining an appropriate sanction.

The SEC is clearly signaling a significantly enhanced enforcement program — enhanced in terms of speed but also in terms of penalties and sanctions. The SEC Enforcement staff listens to speeches and statements of senior officials and, anecdotally, we have been seeing increased SEC staff aggressiveness, shorter deadlines, less process, and the seeking of higher penalties.

CFTC – cryptocurrency and climate change

Over the past several years, the CFTC has aggressively staked out a position in the emergent cryptocurrency markets as well as the accelerating debate regarding climate change-related risk.

With regard to the former, the CFTC has pushed further into the spot markets, enforcing alleged failures to register with the Commission by nascent trading platforms. With regard to the latter, a subcommittee overseen by the now-Acting Chairman of the CFTC, Rostin Behnam, published a report highlighting the risks posed by climate change to financial market stability and carving out a potential role for the CFTC in addressing such risks going forward.

With the transition to the Biden Administration, the CFTC's focus on these areas has only increased, with the agency actively pursuing cryptocurrency trading venues located outside the U.S. for registration failures and other violations linked to making their trading platforms available to U.S. persons. In October of this year, Acting Chairman Behnam noted that recent crypto cases are the "tip of the iceberg." Reflecting the CFTC's continued focus on this perceived threat, enforcement penalties continue to increase in size — most recently measured in the hundreds of millions (USD). Regarding climate change, the CFTC continues to position itself at the center of the debate, for example, in continued discussions about mandating a price for carbon.

Antitrust Enforcement (DOJ and FTC)

A major pillar of President Biden's campaign was to increase and expand antitrust enforcement. With its recent nominees and policy announcements, the Biden Administration has chartered the course for a sharp pivot in U.S. antitrust policy at the federal level and outlined a progressive antitrust agenda that may challenge decades of established practice.

The Biden Administration appointees embody a new progressive approach to antitrust and are known for criticizing established antitrust policy and enforcement. These include Jonathan Kanter, appointed to be Assistant Attorney General for Antitrust at the DOJ; Big Tech opponent Lina Khan, appointed to Chair of the FTC; and White House competition advisor Tim Wu. All three are adherents to the "new Brandeis movement" of antitrust academia — a group originally focused on criticisms of the perceived failure of existing U.S. antitrust laws to curb the power of Big Tech companies — and have all voiced concerns about U.S. antitrust orthodoxy and the lack of monopoly enforcement actions brought by U.S. regulators.

The shift in standards proposed by this group, however, is not limited to Big Tech or even Tech more generally. We can expect much greater scrutiny under existing standards and application of more novel theories to non-tech sectors, particularly in the areas of enforcement. An example of this can be seen in an Executive Order on competition, which was signed by President Biden on July 9, 2021. It aims at reforming competition policy on a broad level, while also targeting certain industries across the American economy. In the Order, President Biden asked federal agencies — both competition agencies and the regulators of the individually targeted industries — to use their powers to increase competition and combat what the Administration perceives as harms to individual consumers caused by the behavior of dominant companies in highly concentrated industries. In particular:

– The Order prompts the DOJ and FTC to action, urging them to challenge previously consummated mergers that may now be found to violate the antitrust laws, to place additional scrutiny on mergers, and generally to enforce antitrust laws vigorously.

– It singles out the markets for labor, healthcare, transportation, agriculture, internet service, technology, and banking and consumer finance for particular focus by competition regulators and other agencies.

– To coordinate implementation of the Order's provisions, it establishes the White House Competition Council, composed of the heads of various federal agencies and chaired by the Special Assistant to the President for Economic Policy and Director of the National Economic Council.

The appointments and Order solidify the Biden Administration's embrace of the antitrust thinking of the progressive wing of the Democratic Party. They serve as an important guidepost for the policies of the new administration, signalling a much more progressive stance on antitrust issues compared to prior administrations.

The full impact of the Biden Administration's antitrust policies will come into even clearer focus once the Order is fully implemented and the new enforcers begin to develop their own cases to test their challenge to antitrust orthodoxy in court. In the meantime, companies should expect extensive reviews of mergers, greater scrutiny of market practices, and more court cases to be brought.

Conclusion

The Biden Administration's push for aggressive enforcement, including its commitment of significant resources to this effort, likely means that companies will increasingly face greater and more frequent scrutiny from regulators.

As such, building and maintaining compliance programs that adequately monitor for, prevent, and remediate misconduct is critical for companies in navigating the more turbulent regulatory environment on the horizon.

Key team members

William Jacobson
Partner – Washington, D.C
Tel +1 202 683 3883
william.jacobson@allenovery.com

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

Julian Moore
Partner – New York
Tel +1 212 610 6309
julian.moore@allenovery.com

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

Noah Brumfield
Partner – Washington D.C.
Tel + 1 202 683 3847
noah.brumfield@allenovery.com

John Roberti
Partner – Washington D.C.
Tel + 1 202 683 3862
john.roberti@allenovery.com

Anthony Mansfield
Partner – Washington D.C.
Tel + 1 202 683 3884
anthony.mansfield@allenovery.com

Gregory Mocek
Partner – Washington D.C.
Tel + 1 202 683 3887
gregory.mocek@allenovery.com

William E. White
Partner – Washington, D.C
Tel +1 202 683 3876
william.white@allenovery.com

Taylor West
Associate – Washington D.C.
Tel + 1 202 683 3867
taylor.west@allenovery.com

"I'm extremely impressed with the quality of their work…It's a very strong team."

Chambers 2021 - Litigation: White-Collar Crime & Government Investigations: The Elite (New York)

"Burgeoning group with an impressive reputation among clients in the financial services sectors, including multinational banks, fintech companies and cryptocurrency trading platforms. Noted for its skilled handling of major FCPA investigations, leveraging its famed global platform to assist with cross-border mandates."

Chambers 2021 - Litigation: White-Collar Crime & Government Investigations (District of Columbia)

David Esseks (NY): "Incredibly experienced, very analytical and a great strategic thinker."
Eugene Ingoglia (NY): "recognized for his sophisticated criminal defense practice, which sees him defend clients facing allegations such as fraud, FCPA violations and criminal tax matters. "
William Jacobson (DC): "regularly acts for clients across a wide range of criminal disputes, and offers notable experience in alleged FCPA violations, as well as serving in corporate monitorship roles..great experience both as a prosecutor and as a former in-house counsel."

Chambers 2021 - Litigation: White-Collar Crime & Government Investigations

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
CS2201_CDD-67155_ADD-100618