Cross-Border White Collar Crime and Investigations Review

2021
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Looking ahead – managing key challenges in 2021</td>
<td>4</td>
</tr>
<tr>
<td>Overview of recent developments by jurisdiction</td>
<td>8</td>
</tr>
<tr>
<td>Australia</td>
<td>11</td>
</tr>
<tr>
<td>Belgium</td>
<td>16</td>
</tr>
<tr>
<td>China</td>
<td>20</td>
</tr>
<tr>
<td>France</td>
<td>25</td>
</tr>
<tr>
<td>Germany</td>
<td>30</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>34</td>
</tr>
<tr>
<td>Netherlands</td>
<td>39</td>
</tr>
<tr>
<td>South Africa</td>
<td>43</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>46</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>52</td>
</tr>
<tr>
<td>United States</td>
<td>57</td>
</tr>
</tbody>
</table>
Introduction

In-house counsel advising on investigations and financial crime risk at large multinational companies have had to contend with a plethora of developments over the past 12 months, not least the additional pressures from Covid-19. Whilst there was a softening of pace on some types of investigations by authorities, most are now back up and running.

More countries are introducing or amending financial crime laws, new types of businesses are being brought into the scope of existing laws, and there is a flow of guidance from enforcing authorities. Investigations lawyers and compliance specialists 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 trends, and highlights the most significant among the current and emerging issues that white collar crime and investigations in-house counsel should prioritise in the year ahead.
Looking ahead – managing key challenges in 2021

We asked our global white collar crime team for their views on key challenges in 2021 for in-house investigations teams and white collar crime lawyers, and how to manage the associated risks.

Understand the evolving risk of 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, 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. This ‘failure to prevent’ model is echoed in the EU’s 6th Anti-money laundering directive (6MLD), whereby criminal liability is extended to corporates where a money laundering offence is committed for their benefit by an individual in a leading position within that corporate or where a lack of supervision or control by such individual has made possible the commission of a money laundering offence.

Any analysis of corporate exposure following allegations of misconduct should factor in the jurisdictions involved, and the risk of corporate (and of course 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. There has been increased guidance from some authorities (in the U.S. and UK) on how they evaluate corporate compliance programmes. 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 accelerated move to remote working.

Increase focus on culture and compliance

Recent 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 the increasingly popular ‘failure to prevent’ type offences. How the policies and procedures are embedded in an organisation is critical to making them effective. The ABAC policies and procedures of a large global company were not enough to save it from a large fine in 2020 as the company had a ‘corporate culture which permitted bribery’. We expect to see even more scrutiny by authorities on ‘tone from the top’ and the tone from within (ie middle management).

How an organisation responds to issues that arise is seen as one of the litmus tests for the culture of an organisation. The identification of incidents through a proper compliance and whistle blower programme, a prompt and objective investigation, and appropriate remediation may be viewed positively by the authorities.
Using, moving and not losing data

More jurisdictions are introducing data protection laws or national security laws which impact data transfer. We expect to see increased data protection enforcement, with large fines, as existing data protection regimes begin to mature.

Those involved with conducting internal investigations will need to:

– ensure protection of personal data, for example when reviewing employee devices and communications;

– check local laws to see whether there are any restrictions on transferring data across borders; and

– keep up to date on how these laws are being enforced – for example, China and Hong Kong have introduced new laws impacting data.

Data analytics offers insights to drive compliance programmes and authorities’ expectations in this regard are increasing. The US DOJ’s recent refinements to its guidance on corporate compliance programmes calls on prosecutors to consider: “Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?”

Compliance teams should consider whether they use data effectively enough to inform the design, implementation and effectiveness of compliance programmes.

Finally, not losing data is a corporate imperative. Companies face hefty fines, and cybersecurity remains a favourite on many authorities’ compliance and enforcement agendas.

Benefit from greater transparency on expectations 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. We see increasing transparency from some authorities on exactly what is expected and in-house counsel should make sure they are aware of guidance (eg from the UK SFO, US DOJ and French PNF) when dealing with the authorities.

Corporate appetite for cooperation will depend on the perceived benefits. In the UK, for example, there are concerns that DPA penalty discounts applied so far for companies that have genuinely self-reported are not sufficiently differentiated from a company that was convicted (following a guilty plea) or did not initially self-report but which was subsequently offered a DPA based on exceptional cooperation during an SFO investigation.

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

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.

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 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.

Understand enforcement risk post Covid-19

Whilst there is some enforcement in most business sectors, there continues to be a higher level of enforcement worldwide, and record breaking fines, against some of the perceived ‘facilitators’ of financial crime such as financial services firms, in a number of areas including in particular AML and the facilitation of tax evasion. We are also seeing increased enforcement involving cryptocurrencies, life sciences and social media.

For all types of business, Covid-19 created the perfect storm for increased financial crime risk owing to the combination of volatile markets, economic pressure to perform, government financial relief packages, compliance staff and technology investment cuts, and home working. Whilst some authorities were impacted by Covid-19, most are now back up and running and will be under pressure to help recoup government finances by seeking out and fining businesses involved in misconduct during the pandemic.

If not already in hand, now is the time for businesses to redouble their efforts on compliance and accurate reporting/disclosures to the markets. Public companies should verify that there are robust policies and procedures in place designed to prevent the misuse of material non-public information and ensure that disclosures adequately address risks created by Covid-19.

Don’t take your eye off intermediaries

The use of intermediaries remains a high corruption risk. Like many previous years, enforcement actions in 2020 related to payments made to third parties concealed as, for example, consultancy fees, sponsorship or charitable donations. The aftermath of the pandemic, and Brexit, may see companies seeing to win work in new jurisdictions, including those that are less developed.

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.
Adapt to stricter AML and CTF regimes

During 2020 we saw many more countries introducing or updating AML laws, even in countries which have historically had weak AML controls. We expect to see continued close scrutiny and large fines in this area, particularly around weak systems and controls. More types of companies and advisors are being brought within the scope of AML and CFT regulation as the law makers try to keep up with the money launderers and those who finance terrorism. The implementation of the EU’s 5th Anti-money laundering directive has bought crypto asset exchange providers, custodian wallet providers, high value art market participants (eg art dealers and freeport operators) and high value property letting agents (previously it was just estate agents) into scope.

More countries are expanding the types of ‘predicate offence’ that can give rise to money laundering. For example, the EU’s 6MLD mandates predicate offences in all Member States to include environmental crimes, tax crimes and cybercrime, as well as more traditional examples such as the trafficking of drugs and humans, fraud and corruption. 6MLD also opens the door to corporate criminal liability for money laundering (see above).

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.

Navigate conflicting laws driven by geopolitics

Multinationals will be familiar with the financial crime laws in jurisdictions where they operate. As more countries amend their financial crime laws it is important that compliance takes account of new requirements. The dynamics of geopolitics at present means that businesses can end up being stuck between conflicting requirements that require delicate navigation (eg sanctions, trade controls, access to data). Businesses are also increasingly popular tools for exerting pressure on human rights abusers – 2020 saw the first EU and UK global human rights sanctions regimes being implemented.

Despite the geopolitics, there is undoubtedly more collaboration between some jurisdictions either informally or formally (such as the new European Prosecutors Office which is expected to bare its teeth in 2021). 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 will impact strategic decisions around interactions with authorities during investigations.

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 recent developments by jurisdiction

**Australia**

Australian regulatory authorities continue to pursue an aggressive enforcement agenda, with consequential increases in the workload of in-house litigation and investigation teams. The current regulatory agenda is being encouraged by a number of factors, including ongoing public criticism and fallout from the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, as well as substantial increases in funding by the Government for key regulators, including the Australian Transaction and Reports Analysis Centre. While the impact of Covid-19 appears to have resulted in a slight pause in the overall level of enforcement action, that trend is likely to be reversed as the Australian economy begins its recovery from the effects of the pandemic. The financial sector continues to draw much of the attention of regulators, but public statements by some regulators, as well as recent reforms, have radically changed the compliance landscape. Boards of all companies, regardless of sector, are under unprecedented pressure to manage conduct risk effectively.

**China**

Despite a tumultuous 2020, China remains on track to complete an ambitious legislative plan, with clear acceleration of major white collar crime legislation and laws that will impact cross-border investigations. 2020 saw a new Securities Law issued, the long-awaited Provisions on the Unreliable Entity List adopted, a new Export Control Law enacted, a significant amendment to the criminal law passed, and the release of a new proposed Personal Information Protection Law that potentially impacts cross-border investigations.

We also observed increased enforcement activity against financial institutions as China’s economy recovered from the pandemic, exemplified by rigorous enforcement against intermediaries for due diligence failures in the capital markets, and against banks and third-party payment institutions for anti-money laundering violations. Following the rapid legislative progress this year, we expect a deluge of enforcement in the years to come.

**Belgium**

The focus of Belgian prosecutors has increased with respect to sanctions, corruption and money laundering. Cyber criminality rising during the Covid-19 pandemic inevitably calls for a prosecutorial response. The College of Attorneys General still encourages the settling of financial and economic criminal cases, which effectively translates into a continuing increase in criminal settlements. Cross-border cooperation between judicial and regulatory authorities is intense, particularly in connection with the transfer of information, both at an EU and global level. Financial intermediaries continue to be targeted in fraud matters, especially in complex cross-border cases. We expect the focus on business responsibility for human rights to increase in 2021.

**France**

France has asserted itself as a hub for white collar crime enforcement in recent years. Spearheaded by the National Financial Prosecutor’s Office (PNF), the white collar criminal enforcement landscape continued to evolve in 2020 towards greater collaboration with overseas enforcement authorities, record-breaking corporate settlements, and some unprecedented large fines.

The PNF came under heavy fire in 2020 after numerous scandals concerning alleged political pressure and aggressive methods. Eric Dupond-Moretti, a former lawyer, and outspoken critic of the PNF’s methods, was chosen to be the new Minister of Justice in July 2020. This criticism may curb the expansion of the French white collar crime enforcement arsenal and push the legislator towards a more balanced rapport between companies and enforcement authorities.
Germany

The criminal enforcement environment in Germany remains robust. Criminal investigations into cum/ex trades are being pursued with high intensity. After the first criminal trial on cum/ex trades ended with convictions of the two defendants and a confiscation against a German bank in March 2020, new trials are currently being prepared or have already started. Besides this, the Wirecard scandal shocked Germany in June 2020 and resulted in criminal allegations and investigations. Furthermore, criminal investigations into the diesel emissions scandal are still affecting many car manufacturers and car components suppliers.

A revised draft bill of a German Corporate Sanctions Act is currently being negotiated in the German Federal Parliament (Bundestag). The Corporate Sanctions Act, expected to be passed by September 2021, will introduce a new system of sanctions for corporate crimes and will impact the conduct of internal investigations.

German authorities are also focusing on the prevention of money laundering and terrorist financing. In line with European legislation, this has led to stricter regulations under the German Money Laundering Act and a draft bill to significantly expand the scope of application of the money laundering offence in the German Criminal Code.

Netherlands

Despite Covid-19, there was no stagnation in the investigation and prosecution of white collar crime in the Netherlands. The Dutch regulators and the Dutch Public Prosecution Service remained focused on the fight against money laundering and corruption. A collective transaction monitoring entity was established by five Dutch Banks to jointly monitor payment transactions for signals that may indicate money laundering. For large Dutch out-of-court settlements, a policy reform entered into force which introduces an assessment by an independent review committee. The Netherlands remains an active jurisdiction for cross-border white collar crime and investigations in 2020 and we expect this trend to continue in 2021.

Hong Kong

Hong Kong saw the enactment of the National Security Law (NSL) in 2020. Corporations or financial institutions are likely to be carrying out detailed and on-going internal analysis to ensure their businesses are NSL-compliant from different perspectives, including anti-money laundering and data protection. Although financial regulatory enforcement actions remain relatively quiet during the Covid-19 pandemic, Hong Kong financial regulators continue to focus on “high-impact” cases and senior management accountability, and thematic reviews to ensure proper market standards are met. The Hong Kong Monetary Authority (HKMA) is expected to implement a mandatory reference checking scheme to address the “rolling bad apples” phenomenon. On the anti-corruption front, the Court of Final Appeal handed down a judgment in line with the modern anti-corruption legislation in challenging secret payments received by agents. Appellate guidance in an uncertain area of law concerning cyber fraud is expected soon.

South Africa

The judicial commissions of inquiry into allegations of corruption and other forms of white collar crime have dominated the South African media cycle. The State Capture scandal remained a key issue in South Africa in 2020, with a number of enforcement actions commencing in 2020. At the same time, the Covid-19 pandemic has seen a wave of new corruption allegations, particularly regarding the procurement of personal protective equipment. In 2021, we expect to see further prosecutions and enforcement action, as well as civil recovery action in respect of misappropriated public funds.
**United Arab Emirates**

The UAE’s approach to white collar crime has come under particular scrutiny over the past year following scheduled reviews by international organisations and a number of high profile cases involving UAE companies.

The UAE has continued to develop and bolster its efforts to tackle white collar crime, both within its “onshore” jurisdictions and within the various “offshore” free zones, most prominently the Dubai International Financial Centre and the Abu Dhabi Global Market, which are subject to the same criminal law but which have their own compliance and regulatory regimes.

Recent legislation has expanded the remit of local regulators beyond financial institutions to cover other high risk sectors of the UAE economy. This has been the case for both onshore regulators (such as the UAE Central Bank) and offshore regulators, such as the DIFC’s Dubai Financial Services Authority and the ADGM’s Financial Services Regulatory Authority.

The implementation and enforcement of this new legislative framework is likely to be a major policy focus for the UAE in the coming years.

**United States**

U.S. enforcement activity was down overall in 2020, with some notable exceptions. The overall scale of white collar criminal prosecutions in 2020 reached a record low. However, FCPA enforcement remained active, there was a burst of enforcement activity in the crypto space, and the size of financial penalties remained substantial. We also saw an increase in activity in antitrust enforcement and sanctions activity. In terms of policy, the DOJ and the SEC have become more transparent about the requirements of cooperation credit and have increased transparency and guidance for FCPA investigations. Enforcement focus was particularly evident with respect to healthcare and biotech industries, social media companies, the financial services industry, and cryptocurrency. The U.S. continues to increase its cooperation and coordination with other authorities as part of the investigation process. While President Trump’s administration winds down, we expect that President elect Joe Biden’s Justice Department will ramp up white collar crime enforcement, returning to a practice of increased scrutiny of corporate wrongdoing.

**United Kingdom**

The UK has high ambitions to fight financial crime, though 2020 saw mixed success for enforcement authorities. While there were three more deferred prosecution agreements (DPAs), including the first with a non-UK company relating to conduct abroad, there were some high-profile failures of corruption prosecutions against individuals whose employers had already entered into DPAs and paid fines for the same alleged conduct. A failed prosecution of a large international bank saw the UK’s rules on corporate attribution examined and reaffirmed, adding fuel to the fire for those seeking reform to make it easier to hold large companies criminally liable. Looking ahead, we expect to see proposals unveiled later this year for reform of corporate criminal liability. There will be increased financial crime risk and enforcement resulting from the perfect storm of market volatility, financial pressures and home working resulting from Covid-19 (eg market abuse, fraud, tax evasion offences). The pressure on UK companies to enter new (perhaps emerging) markets post-Brexit may mean a higher corruption risk.
Australian regulatory authorities continue to pursue an aggressive enforcement agenda, with consequential increases in the workload of in-house litigation and investigation teams. The current regulatory agenda is being encouraged by a number of factors, including ongoing public criticism and fallout from the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (Financial Services Royal Commission), as well as substantial increases in funding by the Government for key regulators, including the Australian Transaction and Reports Analysis Centre (AUSTRAC). While the impact of Covid-19 appears to have resulted in a slight pause in the overall level of enforcement action, that trend is likely to be reversed as the Australian economy begins its recovery from the effects of the pandemic. The financial sector continues to draw much of the attention of regulators, but public statements by some regulators, as well as recent reforms, have radically changed the compliance landscape. Boards of all companies, regardless of sector, are under unprecedented pressure to manage conduct risk effectively.

**Investigations trends/developments**

Each of Australia’s key regulators has been active in 2020, in spite of the effects of the Covid-19 pandemic.

There has been increased enforcement from Australia’s corporate, markets, financial services and consumer credit regulator, the Australian Securities & Investments Commission (ASIC), which can be explained in part by the ongoing effect of recommendations made following the Financial Services Royal Commission. In response to the Financial Services Royal Commission, ASIC adopted a new enforcement approach known as “Why not litigate?”, resulting in more cases being pursued through the courts, rather than by way of settlements or enforceable undertakings. In financial year 2020/2021, enforcement action is budgeted to account for approximately 45% of ASIC’s annual budget of AUD471 million, with another 26% allocated to supervision and surveillance activities.

Australia’s financial crime regulator, AUSTRAC, which is proving itself to be one of Australia’s most successful and prolific regulators, came to an agreement with Westpac Banking Corporation (Westpac) around a AUD1.3 billion penalty arising from 23 million alleged breaches of anti-money laundering laws. This penalty is the largest civil penalty in Australian history.

In order to support its ongoing activities, including its enforcement agenda, AUSTRAC has received a AUD104m funding increase (to be implemented over four years) in the 2020-2021 Federal Budget, including an additional 67 new staff. In addition to strengthening its enforcement activities, the increased funding is intended to support the delivery of a new modern reporting system that better assists reporting entities to fulfil their compliance obligations, and allow more resources to be dedicated to proactive regulation, education and outreach to support industry.

In its 2020 statement of enforcement priorities, Australia’s competition regulator, the Australian Competition and Consumer Commission (ACCC), continued to place a focus on cartel conduct and other anti-competitive practices that involve “Australians, Australian business or entities...
carrying on business in Australia’. It has placed particular emphasis on competition and consumer issues relating to digital platforms and has focused on investigations involving digital platforms allegedly misleading consumers about the collection and the use of their personal data. The ACCC has also been looking closely at the pricing and selling practices of essential services, particularly in relation to electricity and telecommunications.

The ACCC is continuing in its prosecution of a high-profile criminal cartel case against two global investment banks, one of Australia’s largest domestic banks, and six of their senior executives, relating to a capital raising in 2015 and four phone calls that occurred among the defendants over a weekend.

On 1 January 2020 the Australian Sanctions Office was created within the Department of Foreign Affairs and Trade. The enforcement of sanctions in Australia is criminal, not civil. Enforcement of Australia’s sanctions laws has witnessed a steady increase in recent years, with a number of criminal prosecutions currently working their way through the court system, including one case involving the alleged export of nickel alloys to Iran (which is a banned export on the basis that it could contribute to Iran’s nuclear programme), and another prosecution in which an individual has been charged with breaching United Nations sanctions for the supply of products related to the proliferation of weapons of mass destruction to North Korea.

**Significant law reforms impacting corporate criminal liability**

The Australian Law Reform Commission’s (ALRC) Final Report on Corporate Criminal Responsibility (see here) (ALRC Corporate Criminal Responsibility Report) was made public on 31 August 2020. The ALRC inquiry into corporate criminal responsibility in Australia followed on from widespread concerns that corporations, and senior officers within those corporations, are not adequately held to account for serious corporate misconduct. The report makes a number of recommendations, with the stated intention of better aligning corporate liability with corporate culpability, and reducing the multiplicity and complexity of current laws relevant to corporate misconduct, many of which the ALRC says lack a principled basis and are often duplicative. Highlights from the ALRC’s findings are:

– prosecutions of corporations, relative to individuals, are extremely rare, even in heavily regulated sectors where corporations are most active;

– prosecutors withdraw a significantly higher number of charges against corporations than they withdraw against individuals for corporate crimes, suggesting that existing laws present real difficulties in prosecuting corporations;

– Commonwealth law contains a variety of complex mechanisms for attributing criminal responsibility to corporations, but should instead contain just one standard mechanism. In order to focus squarely on corporate blameworthiness, fault should be attributed to corporations with a poor compliance culture. A corporation should be able to avoid liability by demonstrating it took reasonable precautions to prevent misconduct (ie by demonstrating an absence of corporate fault);

– there is concern that the paucity of corporate criminal prosecutions, and regulators’ frequent reliance on civil penalty provisions, have led to a mind-set that the penalties imposed are little more than a cost of doing business;

– new penalty and sentencing options should be introduced to empower courts to take into account the impacts on third parties, and to punish those most involved in the wrongdoing.

Amendments to Australia’s anti-money laundering legislation were passed in December 2020 to simplify and clarify provisions relating to customer due diligence, correspondent banking and tipping off. See here for our discussion of the amendments when they were introduced to parliament in 2019, and our discussion of the passing of the amendments by parliament here.

In the coming months it is likely the Crimes Legislation Amendment (Combating Corporate Crime) Bill 2019 will be passed. This legislation will introduce a “failure to prevent bribery” offence similar in style to the s7 Bribery Act 2010 office, as well as a deferred prosecution agreement scheme.
Internal investigations – key developments

In the current enforcement environment, ASIC is heavily scrutinising claims for privilege in the context of regulatory investigations, particularly in circumstances where sufficient details supporting the basis of the claim are not provided from the outset.

The ALRC report (see above) highlights the importance of conducting appropriately tailored internal investigations, and the potential for hindsight scrutiny of the adequacy of those processes by external parties (eg prosecutors, courts) in the context of regulatory enforcement action. The ALRC Corporate Criminal Responsibility Report recommended that the Crimes Act 1914 (Cth) should be amended to require a court to consider a multitude of factors when sentencing a corporation, including “any measures that the corporation has taken to reduce the likelihood of its committing a subsequent offence, including: (i) internal investigations into the causes of the offence; (ii) internal disciplinary action; and (iii) measures to implement or improve a compliance program”. In-house teams should consider taking steps to ensure they have, or source externally, appropriately qualified expertise to conduct such investigations.

Sectors targeted by law reforms or enforcement action

The financial services sector remained a focus for enforcement action during 2020 across multiple regulators. The AUD1.3bn civil penalty imposed on Westpac for breaches of Australia’s anti-money laundering laws marked the largest civil penalty in Australian history. AUSTRAC’s Chief Executive Officer, Nicole Rose, indicated that AUSTRAC will remain focused on the financial sector in 2021, stating “our role is to harden the financial system against serious crime and terrorism financing and this penalty reflects the serious and systematic nature of Westpac’s non-compliance”.

This is not to say that AUSTRAC is only focused on the financial services sector; AUSTRAC has publicly indicated that it is considering enforcement action against a major non-banking institution, with a view to commencing proceedings during the 2020/21 financial year.

In its Enforcement Update¹, ASIC stated that it is prioritising:

1. Financial Services Royal Commission referrals and case studies.
2. Misconduct related to superannuation and insurance.
3. Cases that engage ASIC’s new powers or provisions that now carry penalties or higher penalties.
4. Illegal phoenix activity.
5. Auditor misconduct.
6. New types of misconduct (eg those carried out online or using emerging technologies).

In addition, ASIC has stated that it will always prioritise:

1. Significant market misconduct.
2. Misconduct that is serious either by its nature or extent of harm, or that involves a large market participant or licensed entity.
3. Misconduct that involves a high risk of significant consumer harm, particularly involving vulnerable consumers.
4. Misconduct by individuals, particularly criminal conduct or government failures, at board or executive levels.

Separately, as the impact of Covid-19 began to be felt across the Australian economy, ASIC stated in March 2020 that it was recalibrating its regulatory priorities. It said it would maintain its enforcement activities but would target “action necessary to prevent immediate consumer harm, egregious illegal conduct and other time critical matters”. ASIC has also stated that it has implemented a set of pandemic-related enforcement priorities to guide its response to misconduct associated with the pandemic. Those priorities aim to address misconduct arising from behaviour seeking to exploit the pandemic environment, opportunistic misconduct (such as scams, unlicensed misconduct, and misleading and deceptive advertising), failures to disclose materially negative information, opportunistic and misleading market announcements made to the ASX, and egregious governance failures.

¹ Report 666, September 2020
Cross-border coordinated enforcement activity

Australian regulatory authorities regularly collaborate with their overseas counterparts. For example, the Australian Federal Police (AFP) has been a member of the International Foreign Bribery Taskforce since 2013 and has worked on several matters with its other members (including the UK National Crime Agency and the U.S. Federal Bureau of Investigations (FBI)), a number of which are ongoing.

In a recent example of cross-border cooperation and enforcement, in November 2020 the AFP arrested a former senior executive of Leighton Offshore Pty Ltd for foreign bribery offences, engaging in conduct to falsify books, and knowingly providing misleading information, all in relation to a plan to bribe Iraqi officials in exchange for oil pipeline contracts. The AFP stated that it had worked in close collaboration with the UK’s Serious Fraud Office, the U.S. Department of Justice, and the FBI. The AFP also stated that it had obtained evidence from ten countries, and provided evidence to help foreign law enforcement partners secure guilty pleas to foreign bribery charges.

Financial crime issue predictions for 2020

Responding to greater enforcement activity and improved enforcement powers of regulators is a principal challenge for corporates operating in Australia at present. As noted above, regulators have received major additional funding to undertake this enforcement activity. The increased funding has led to greater cooperation and coordination between regulators, as well as an increase in concurrent regulatory investigations (where the conduct falls within overlapping regulatory ambits). As a result, the Australian legal and compliance market is experiencing a considerable skills shortage, making it even more difficult to staff the increased workload.

Further, pressure on boards to adequately monitor non-financial risks, as well as the recent imposition of several new obligations that are broadly worded or principle-based (such as the Financial Accountability Regime, which will replace the Banking Executive Accountability Regime that commenced on 1 July 2019 and which is designed to further increase transparency and accountability and improve risk culture and governance by imposing a range of accountability obligations on an array of entities and their senior executives), has necessitated the development of more mature compliance systems. This has led to an increase in change projects designed to identify and manage such risks, and a greater investment in consultants with expertise in regulatory compliance, as well as corporate culture and governance.

General Counsel will need to be particularly focused on the use of IT systems and infrastructure to address conduct risk and compliance processes. Such systems can be critical for meeting the regulatory obligations of large institutions, however breakdowns in those systems or related processes can lead to large-scale data breaches or systemic non-compliance with the regulations they were intended to meet.
Jason Gray assists clients on a variety of matters, including investigations and compliance with Bribery and corruption investigations, Money Laundering Investigations, Sanctions investigations, Cyber and Data investigations, Fraud investigations, Tax litigation and investigations, Securities investigations, regulation. A client appreciates the depth of his knowledge, saying: “He’s obviously well versed in the subject matter and always makes sure that we get the right questions and the input that we need to provide.”

“We’re a very happy customer – they did very good work, they were focused on our needs, very available and did very good work.”

-Chambers Asia Pacific 2021

Key team members

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

**Edward Einfeld**  
Senior Associate – Sydney  
Tel +612 9373 7753  
edward.einfeld@allenovery.com

**Jessica Ji**  
Senior Associate – Sydney  
Tel +612 9373 7576  
jessica.ji@allenovery.com
Belgium

The focus of Belgian prosecutors has increased with respect to sanctions, corruption and money laundering. Cyber criminality rising during the Covid-19 pandemic inevitably calls for a prosecutorial response. The College of Attorneys General still encourages the settling of financial and economic criminal cases, which effectively translates into a continuing increase in criminal settlements. Cross-border cooperation between judicial and regulatory authorities is intense, particularly in connection with the transfer of information, both at an EU and global level. Financial intermediaries continue to be targeted in fraud matters, especially in complex cross-border cases. We expect the focus on business responsibility for human rights to increase in 2021.

Investigations trends/developments

We continue to see an increase in enforcement action for (i) corruption; (ii) cyber criminality; (iii) economic and financial crime, including tax fraud; (iv) terrorism; and (v) human trafficking offences.

While overall crime statistics are decreasing, cybercrime is firmly on the rise: 2019 saw a 30% year on year increase in reported cybercrimes, a trend that only accelerated with the outbreak of the Covid-19 pandemic in early 2020 (in particular for online fraud and ransomware attacks). Fighting cybercrime continues to be a priority for Belgian authorities, who increasingly engage in cross-border enforcement and information exchange. Also, we see a trend in Belgian law enforcement actively cooperating with companies seeking to recover systems and data after a cyber-attack.

Significant law reforms impacting corporate criminal liability

Seven months after the EU deadline passed, on 20 July 2020, Belgium finally implemented the Fifth AML Directive (2018/843/EU). As a result, several key amendments were made to the existing Belgian AML Act, including the introduction of new “obliged entities”.

The implementation of a Belgian UBO register (another requirement under the AML Directives) had already occurred in October 2018 but was initially subject to a “tolerance period” granted by the Belgian Federal Public Finance Department. The “tolerance period” ended on 31 December 2019, and from 1 January 2020 breaches of UBO-related obligations may result in criminal and/or administrative penalties.

On the sanctions and embargoes front, in addition to criminal liability, breaches of EU sanctions are now also subject to administrative fines by the Belgian Ministry of Finance and Economy, as are breaches of the EU Blocking Regulation that prohibits EU entities or individuals from complying with certain U.S. sanctions and export controls. Along with the first listings under the EU cyber sanctions regime and reports on an impending revision of the sanctions landscape under Belgian law, we are expecting greater enforcement and corporate liability to follow.
Internal investigations – key developments

There is no regulatory or statutory framework in Belgium specifically dealing with internal investigations. Corporates are in principle free to conduct internal investigations in parallel with criminal or regulatory investigations without any positive duty to disclose the results of the internal investigation. However, general GDPR requirements apply and must be taken into account.

The authorities may seize materials produced in the process of an internal investigation in the context of a search, however, these materials may be protected by legal privilege if an attorney-at-law is involved or, under certain conditions, if produced and sent by in-house counsel.

Sectors targeted by law reforms or enforcement action

As an unexpected extra to implementing AMLD5 into Belgian law (see above), the Belgian legislator extended the scope of the Belgian AML Act to the professional football sector in Belgium. As a result, football clubs, player agents and the Royal Belgian Football Association are now subject to the Belgian anti-money laundering framework. This triggered an outright revolution in the sector. This change was introduced at the very last hour in the legislative process, reportedly in response to the 2018 Belgian football fraud scandal that is currently the subject of an extensive criminal investigation into private corruption and money laundering (in addition to other criminal investigations recently initiated involving certain football clubs and player agents).

In addition to this specific reform, because of the opacity of money flows in complex cases, we see a continued focus by Belgian prosecutors on financial intermediaries when investigating and prosecuting fraud matters (often based on aiding and abetting).

Cross-border coordinated enforcement activity

We have seen an increase in cross-border fraud investigations coordinated at EU-level by the European Anti-Fraud Office (OLAF) and then handed over to Belgian authorities with a recommendation to prosecute. Because OLAF has no prosecutorial powers, it needs to rely on local authorities for repressive measures. A new regulation is being developed to ensure smooth cooperation between OLAF and the European Public Prosecutor’s Office (EPPO) (expected to become operational at the beginning of 2021) and to enhance the effectiveness of OLAF’s investigations. We expect a rise of OLAF-coordinated cross-border investigations as a result of these developments, especially given the strong stance taken by the EU regarding the protection of its financial interests.

Financial crime issue predictions for 2020

Detecting and preventing corrupt practices, money laundering, sanctions/embargoes and cyber security will stay high on the agenda for 2021.

We also expect business responsibility for human rights to be in the focus of GCs over the next year. Companies operating in the EU should be on the lookout for the first listings under the recently adopted EU global human rights sanction regime, which will add yet another layer to the sanctions framework they must comply with. The EU Commission is also expected to publish a draft directive on mandatory human rights and environmental due diligence in Q2 2021, which will have far-reaching consequences for Belgian businesses given the absence so far of any corporate due diligence obligations under Belgian law.
2020 – Practice

“The white collar crime and investigations practice at Allen & Overy LLP benefits from ‘a hands-on and available team, that never loses focus on key topics’. The group attracts praise for providing ‘very concise advice’ on a range of matters, from due diligence issues, compliance programmes and internal investigations to regulatory investigations and criminal prosecutions. Work highlights include acting for premier league soccer club KV Mechelen in criminal, disciplinary and civil proceedings in Belgium and Switzerland relating to allegations of match fixing, bribery and money laundering.”

Ranked Tier 1 – 2020, Legal 500, Fraud and White collar Crime

2020 – Individual – Joost Everaert

“Clients praise the ‘solution-oriented’ lawyer for being ‘able to give quick legal advice’ and displaying ‘a particularly good knowledge of our industry’.”

Ranked Tier 1 – 2020, Chambers Europe, Dispute Resolution: White collar Crime

“The team is led by litigator Joost Everaert, who frequently advises on criminal risk, compliance matters and investigations, and is instructed by defendants and claimants in criminal proceedings and negotiations with prosecutors.” […]

“Joost Everaert is great and never loses his calm.”

Ranked in the “Hall of Fame” – 2020, Legal 500, Fraud and White collar Crime

2020 – Individual – Nanyi Kaluma

“Counsel Nanyi Kaluma is particularly experienced in cross-border bribery and money laundering investigations.”

Ranked as “Rising Star” – 2020, Legal 500, Fraud and White collar Crime
2019 – Practice

“Allen & Overy LLP’s group has been handling cases of money laundering, tax fraud, embezzlement, and cybercrime, among other areas. Regulatory investigations and compliance matters are additional core strengths.”

Ranked Tier 1 – 2019, Legal 500, Fraud and White collar Crime

2019 – Individual – Joost Everaert

“Interviewees enthuse that he is ‘a very thorough litigator,’ while others describe him as ‘an extremely bright mind’.”

Ranked Tier 1 – 2019, Chambers Europe, Dispute Resolution: White collar Crime

Ranked as “Leading Individual”

2019, Legal 500, Fraud and White collar Crime

2019 – Individual – Nanyi Kaluma

“Nanyi Kaluma is noted for her expertise in cross-border money laundering and bribery investigations.” –

Ranked as “Next Generation Lawyer”

2019, Legal 500, Fraud and White collar Crime

Key team members

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

Nanyi Kaluma
Counsel – Brussels
Tel +32 2 780 26 38
nanyi.kaluma@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

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

Mathilde Vandormael
Trainee – Brussels
Tel +32 2 780 2522
mathilde.vandormael@allenovery.com
Despite a tumultuous 2020, China remains on track to complete an ambitious legislative plan, with clear acceleration of major white collar crime legislation and laws that will impact cross-border investigations. 2020 saw a new Securities Law issued, the long-awaited Provisions on the Unreliable Entity List adopted, a new Export Control Law enacted, a significant amendment to the criminal law passed, and the release of a new proposed Personal Information Protection Law that potentially impacts cross-border investigations.

We also observed increased enforcement activity against financial institutions as China’s economy recovered from the pandemic, exemplified by rigorous enforcement against intermediaries for due diligence failures in the capital markets, and against banks and third-party payment institutions for anti-money laundering (AML) violations. Following the rapid legislative progress this year, we expect a deluge of enforcement in the years to come.

Investigations trends/developments

**Strengthened enforcement against financial institutions during the economic recovery from the pandemic**

(i) Increasing focus on misrepresentation by issuers and due diligence failures by intermediaries

In 2020, PRC regulators cracked down dramatically on securities-related misconduct, in particular misrepresentation by issuers and due diligence failure by intermediaries. According to Securities Daily, by 2 November, the China Securities Regulatory Commission (the CSRC) and its local branches issued 219 administrative penalties in total, including: (i) 82 alleged misrepresentation cases by issuers, an increase from 29 in 2019; and (ii) 106 cases against intermediaries, most relating to due diligence failures by underwriters, a significant increase from 11 in 2019.

(ii) Reinforced AML enforcement, mainly targeting banks and payment institutions

China has been refining its AML regime over the years to catch up with international standards. The AML regime extended its reach from traditional banking institutions to insurance companies and securities firms in 2007 (when China joined the Financial Action Task Force), and to payment institutions in 2012.

This year, the People’s Bank of China, the main regulator responsible for AML enforcement, greatly stepped up its enforcement efforts. By July 2020, the number of penalties under the PRC Anti-Money Laundering Law already outnumbered the entirety of penalties in 2019. By 30 September 2020, 456 AML penalties had been published, with total fines of approximately RMB493m. Banks and payment institutions remain the main targets of enforcement actions. The most commonly seen bases for punishment were failure to perform customer identification obligations and failure to submit large or suspicious transaction reports.
Significant drop in anti-bribery and anti-corruption (ABAC) cases

Compared to 2019, 2020 saw a drop in the number of published adjudications for criminal bribery cases under the Offence of Offering Bribes by an Entity and the Offence of Offering Bribes to a Non-state Functionary under the PRC Criminal Law (the Criminal Law). According to the Wolters Kluwer legal database, as at 11 November, 2020, there were: (i) 126 first-instance cases under Article 393, a significant decrease from 391 in 2019; and (ii) 84 first-instance cases under Article 164, a slightly smaller decrease from 140 in 2019.

Similarly, the number of published administrative penalty decisions under Article 7 of the PRC Anti-Unfair Competition Law (which provides the basis for administrative liability for “commercial bribery”) dropped from 42 in 2019 to 21 in the first 11 months of 2020. Nearly half of the 21 cases involved the life sciences industry.

Is the Chinese government loosening its grip on the anti-corruption campaign? We don’t think so. A number of cases still involved senior officials, including provincial party secretaries, a deputy provincial governor, and a vice-chief of a higher people’s court, each removed from their positions and sentenced for corruption. Much of the decline in ABAC cases has been attributed to the diversion of regulators’ attentions during the pandemic, and there has been little indication that the anti-corruption campaign has diminished as a policy initiative. Indeed, at the very tail-end of 2019, China armed its newly established watchdog, the National Supervisory Committee (the NSC), with greater powers designed to reduce its collaboration with the judicial system. On 30 December 2019, the Supreme People’s Procuratorate (the prosecutor) revised its Criminal Procedure Rules to make clear the process for transfer of cases from the NSC for criminal prosecution.

Significant law reforms impacting corporate criminal liability

Significant revisions to the Criminal Law

Adding or revising more than 40 provisions, the 11th Amendment of the Criminal Law is one of the most significant changes since the Criminal Law’s enactment in 1997. These amendments cover such areas as financial crime, corruption, workplace safety, food and drug safety, juvenile liability, infringement of corporate properties, and public health. There are key changes to money laundering, market manipulation, fraud and private sector embezzlement, and increased sentences and fines for securities fraud, bribery, and AML.

New export control regime

The PRC Export Control Law (the ECL), initially proposed in 2017, took effect on 1 December 2020. It replaces a set of non-systematic export control measures under the Foreign Trade Law and its administrative regulations, and sets up a new framework for China’s export control regime.

The ECL applies to export controls over dual-use items, military items, nuclear items, and other items relating to national security and interests. These items include products, technologies, and services.

Under the ECL, regulators are empowered to create export control lists, decide export control measures, issue export permits, conduct investigations, and punish violations. Detailed regulations for the implementation of the export control regime will be made at a later date.

Violation of the ECL can lead to serious consequences, including confiscation of illegal income, a fine as high as 20 times the amount of the illegal revenue, suspension of operations, and revocation of relevant export qualifications. There is also personal liability for individual violators, including the potential for a lifetime ban on export activities.

The ECL expressly provides for extraterritorial reach, stating that it applies to “any entity or individual” outside China that violates the ECL and endangers the national security and interests of the PRC, or hinders the fulfilment of such international obligations as non-proliferation.

The ECL also allows the state to employ reciprocal measures against a country or region that is abusing its own export control measures and in so doing is harming China’s national security and interests. This introduces the possibility that regulators may take actions beyond the general framework of the ECL.
The Unreliable Entity List Regime and transactions with foreign entities

The Provisions on the Unreliable Entity List (the UEL Provisions) were released on 19 September 2020. They target foreign enterprises, organisations, and individuals that: (1) endanger the sovereignty, security, and national interests of China; or (2) suspend normal business transactions with, or take discriminatory measures against, Chinese enterprises and organisations, or in violation of normal market transaction principles. The UEL Provisions are widely perceived as China’s response to the U.S. increasing its use of its sanction regime against Chinese citizens and enterprises, and is a tool to protect China’s national, economical, technological, informational, and supply-chain security.

The Provisions are implemented by a cross-departmental working mechanism under the State Council, which also determines the restrictions and punishments against listed entities (including restrictions or prohibitions on China-related export/import activities, investment in China, entry into the territory of China, residential permits/qualification to stay in China, and imposition of fines).

A foreign entity that is listed will need to consider the procedure for ‘delisting’, which states potential rectification steps.

The UEL Provisions add to China’s leverage over multinational companies, including those that choose to abide by U.S. sanction laws where China’s national interests are at stake. There is a risk that multinational companies may find themselves in a dilemma where compliance with the laws of both countries becomes challenging.

The ECL and the UEL Provisions are two pillars of China’s sanctions and embargo regime. The ECL concerns export activities of controlled items, while the UEL Provisions capture broader transactions with foreign entities that pose a more direct threat to China’s national interests. While the ECL is actually a law, the UEL Provisions are departmental regulations. While both rules were adopted as defensive tools, the Chinese government may increasingly use them for proactive engagement when projecting influence internationally.

New Securities Law – class actions and long-arm jurisdiction

The new PRC Securities Law, which took effect on 1 March 1 2020, provides more severe punishment for market manipulation and insider trading, enhances issuers’ responsibilities for information disclosure, and strengthens enforcement against due diligence failures and other misconduct by intermediaries. For instance, under the 2014 Securities Law, an institutional market manipulator could receive a fine of up to five times its illegal income, and an individual manipulator could receive a fine of up to RMB 600,000. Under the new Securities Law, fines have been increased to ten times the illegal income, and up to RMB5m, respectively. Two specific developments are worth noting:

- **New ‘opt-out’ class action system for securities-related cases:** an investor protection organisation entrusted by more than 50 investors can represent all relevant securities holders in a civil litigation. All securities holders confirmed by the securities depository and clearing institution will become plaintiffs automatically, except for those who affirmatively express the intention to be excluded.

- **The long-arm jurisdiction clause:** the new Securities Law provides: “Any offering or trading of securities outside of the territory of the People’s Republic of China, when disturbing the market order within the People’s Republic of China and harming the legitimate rights and interests of domestic investors, shall be dealt with and subject to liability according to the applicable provisions of this Law.” (Long-Arm Clause). CSRC’s reaction to the Luckin case suggests that the Long-Arm Clause is more likely to be applied to overseas activities that directly impact the Chinese domestic securities market, such as malicious manipulation or shorting of the Chinese market.
Internal investigations – key developments

Transmission of personal data abroad in the context of investigations

A draft Personal Information Protection Law was released in October 2020 (the draft PI Protection Law) and explicitly requires all “personal information processors” to submit applications with the relevant authorities where personal information is expected to be provided abroad for international judicial assistance or administrative enforcement assistance.

The blocking provision of the Law of the People’s Republic of China on International Criminal Justice Assistance (the ICJA Law), previously enacted in October 2018, provides that no authorities, organisations, or individuals in foreign countries may carry out criminal proceeding activities within China, and no authorities, organisations, or individuals within China may provide evidentiary materials or criminal judicial assistance to any foreign countries, without the consent of the competent authorities of China. After two years, there is no indication that Chinese authorities have enforced this provision. The PI Protection Law suggests, however, that the Chinese government is considering developing other, more direct measures to block the extraterritorial reach of foreign countries.

Sectors targeted by law reforms or enforcement action

As noted, in the ABAC area, the life science industry remains a primary focus of enforcement.

In capital markets, the due diligence failures of intermediaries have become a new focus of regulatory investigation and enforcement, especially for small and medium-size brokers and underwriters.

In the AML regime, the regulator has expanded enforcement against banks and third-party payment institutions.

Cross border coordinated enforcement activity

Enforcement collaboration between China and Western jurisdictions

The news in 2020 has largely focused on a deterioration of relationships between China and a number of Western jurisdictions, the United States in particular. Yet there are at least some indications that good-faith enforcement collaboration still takes place. In April 2020, when Luckin Coffee Inc., a China-based NASDAQ-listed company, announced findings of an estimated RMB2.2bn (USD310m) in false sales, the CSRC immediately expressed its disapproval of “all forms of fraud by listed companies”. The CSRC stated publicly that it had “proactively initiated communications with the SEC with regard to possible investigation into Luckin Coffee”, and expressed “readiness to cooperate fully with the SEC under the IOSCO Multilateral Memorandum of Understanding”.

Yi Huiman, the Chairman of CSRC, also stated that CSRC had provided the SEC and the Public Company Accounting Oversight Board (PCAOB) with audit working papers of 14 Chinese companies listed on the U.S. securities markets. According to Yi, since 2019, CSRC had made several proposals to PCAOB regarding a “joint inspection” approach for audit supervision, although U.S. authorities had not returned positive feedback.

However, as China continues to wrangle with Western jurisdictions over tariffs, sanctions, high profile cases such as the detention of Huawei’s Chief Financial Officer, and high-profile legislation such as the U.S. Holding Foreign Companies Accountable Act, the potential for further cross-border enforcement collaboration appears bleak, at least in the near future.

Enforcement collaboration between mainland China and Hong Kong

Given that many international financial institutions rely on their Hong Kong presence to access China’s securities markets, financial regulators such as the CSRC have expanded cooperation with their counterparts in the Hong Kong Securities and Futures Commission, and have asked the latter to pass along requests for document production and to conduct interviews for CSRC investigations. We expect that such cooperation will become more frequent as China exerts its sovereignty over the Special Administrative Region.
Financial crime issue predictions for 2020

In anticipation of the final enactment of the Personal Information Protection Law, coupled with the existing obstacles in the ICJA Law limiting cross-border information transfer for criminal judicial assistance purposes, we can expect cross-border data transfer for the purposes of investigations to be subject to stricter scrutiny, particularly when the data requests are responsive to requests from foreign regulators. In-house legal and investigation teams may face a dilemma where it becomes increasingly difficult to comply with both requests from foreign regulators and PRC blocking statutes at the same time.

The expedited roll-out of China’s sanctions regime also has the potential to substantially impact operations of multinational companies that do business in China, particularly before implementing regulations are made. It remains to be seen whether China’s flurry of legislation in this area is the beginning of a comprehensive, and well-thought-out legal regime, or a short-term response to the current political climate.

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

Key team members

Eugene Chen
Registered Foreign Lawyer – Hong Kong
Tel +852 2974 7248
eugene.chen@allenovery.com
Profile link: https://www.allenovery.com/en-gb/global/people/Eugene_Chen

Jane Jiang
Partner – Shanghai
Tel +86 21 2036 7018
jane.jiang@allenovery.com
Profile link: https://www.allenovery.com/en-gb/global/people/Jane_Jiang

Yihan Zang
Senior Associate – Shanghai
Tel +86 21 2036 7142
yihan.zang@allenovery.com
Profile link: https://www.allenovery.com/en-gb/global/people/Yihan_Zang

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

France has asserted itself as a hub for white collar crime enforcement in recent years. Spearheaded by the National Financial Prosecutor’s Office (PNF), the white collar criminal enforcement landscape continued to evolve in 2020 towards greater collaboration with overseas enforcement authorities, record-breaking corporate settlements, and some unprecedented large fines.

The PNF came under heavy fire in 2020 after numerous scandals concerning alleged political pressure and aggressive methods. Eric Dupond-Moretti, a former lawyer, and outspoken critic of the PNF’s methods, was chosen to be the new Minister of Justice in July 2020. This criticism may curb the expansion of the French white collar crime enforcement arsenal and push the legislator towards a more balanced rapport between companies and enforcement authorities.

Investigations trends/developments

2020 saw a continued shift in French judicial and prosecution culture to a more collaborative and transactional approach. French-style deferred prosecution agreements (known as CJIP – Convention Judiciaire d’Intérêt Public) have become more common in matters ranging from corruption to tax evasion, and have resulted in the payment of significant fines, particularly by banks.

The success of CJIPs encouraged the legislator to expand the scheme to include tax fraud. In late 2019 a global technology company was one of the first companies to settle a tax fraud dispute with a CJIP. It agreed to pay EUR500m over the alleged existence of a permanent establishment of its Irish entity on French soil.

The CJIP is likely to be extended and amended further to include environmental offences and laundering the proceeds of corruption or of influence peddling. In addition, companies seeking to settle a CJIP may no longer be required to recognise the disputed facts and accept their criminal nature, making it increasingly interesting from a reputational standpoint.

This collaborative and transactional approach must not be confused with clemency, as prosecutors have sought, and judges have handed down, unprecedented fines. In 2019 French judges ordered a large Swiss bank to pay a record EUR3.7bn fine for illicit banking solicitation and aggravated money laundering of the proceeds of tax evasion (the ruling is currently under appeal). In January 2020, the National Financial Prosecutor’s Office (the PNF), along with its UK and U.S. counterparts, entered into a record-breaking CJIP with a large aerospace company (over EUR3.6bn) for alleged acts of bribery and corruption.
Significant law reforms impacting corporate criminal liability

A recent ruling by the French Supreme Court (Cour de Cassation)\(^4\) found that, in the event of a merger of certain public limited liability companies, the acquiring company may be convicted of criminal wrongdoing committed by the acquired company prior to the merger. This stark departure from previous French case law has serious implications for mergers. Companies are likely to want to undertake an even greater level of pre-acquisition due diligence, plus negotiations of disclosure and warranty clauses are likely to take longer. The new ruling applies to mergers that take place after 25 November 2020.

There is a further move towards encouraging companies to voluntarily disclose wrongdoing. New guidelines for prosecutors on international bribery were issued in June 2020 (known as “Circulaire Belloubet”) and state that:

– to benefit from “some form of leniency as to the methods of prosecution likely to be undertaken by the PNF”;

– as provided for in the Sapin II statute, any corporate “residing usually, or exercising all or part of [their] economic activity, in French territory” may be prosecuted by the PNF.

For tax evasion and tax fraud offences, the French legislator had already moved towards a voluntary self-disclosure regime. In 2019, it launched the SMEC programme, a “corporate tax compliance service”, which allows companies to self-report irregularities in their tax situation in return for reduced penalties and no criminal conviction, provided that no tax, administrative or legal proceedings are underway. The programme is still in its early days, and has yet to yield any concrete results (17 cases are currently being examined), but it sets the tone for what is expected from corporates concerning cooperation with tax authorities.

Internal investigations – key developments

The Circulaire Belloubet encourages internal reporting and investigating of corrupt practices, however there are still some difficult issues to contend with at the internal investigation stage. The scope of privilege is still much debated in France. The PNF’s 2019 CJIP guidelines provide that “not all documents of an internal investigation are covered by professional secrecy laws”. In June 2020 the French National Bar Association (CNB) set out guidelines concerning internal investigations, which state that internal investigations conducted by lawyers should be covered by professional secrecy laws, as they are an integral part of the rights of the defence. Case law has not yet clarified the issue, although it tends to favour a more restrictive view of client/attorney privilege, in considering only documents drafted in preparing a client’s criminal defence to be covered.

The issue of confidentiality of internal investigation documents is particularly important given that, in the event of failed negotiations for a CJIP, the PNF provides no guarantee that the documents exchanged during the investigation and negotiation will not be used in further proceedings. Administrative case law is more protective of attorney/client privilege. It bars administrative regulators such as the French equivalent to the Financial Conduct Authority (“Autorité des Marchés Financiers”, known as the AMF), from seizing the work product of internal investigations conducted by lawyers or any correspondence exchanged between a lawyer and client, in particular any legal advice drawn up by the lawyer for the client.

An additional issue in internal investigations is movement of data. Those undertaking an internal investigation must consider whether information may need to be disclosed to a foreign enforcement authority:

– in its 2020 guidelines, to avoid violating GDPR rules, the CNB recommends carrying out a data protection impact assessment prior to an internal investigation, and notifying relevant individuals that their data could be used for litigation purposes; and

– the CNB guidelines encourage lawyers to advise foreign authorities of the requirements set out in the French Blocking Statute, and to negotiate the scope of disclosure requests. To avoid any unnecessary transfer of data outside of French territory, the guidelines also recommend appointing forensic services that can host the data in France while still allowing foreign authorities access to review it.

\(^4\) Cass. Crim., 25 November 2020 n°8-86.955
Sectors targeted by law reforms or enforcement action

The Circulaire Belloubet is a new and emphatic assertion of French criminal jurisdiction over foreign companies with a presence in France, generating a criminal exposure for all activities with a French nexus. The Sapin II statute provides that French law is applicable to any instance of corruption or bribery committed abroad by persons or corporate entities “residing usually, or exercising all or part of [their] economic activity, in French territory”. However, the Circulaire Belloubet specifies that the legislator intended this to be understood broadly, thus encompassing corporations “with a subsidiary, branches, commercial offices or other office operating in France, even if these would not have their own legal personality”.

The PNF is therefore encouraged to investigate bribery offences committed anywhere around the world as long as the corporate having committed the wrongdoing conducts some of its business in France or has a representative office there. The Circulaire Belloubet seems to push the PNF towards a more proactive approach particularly against foreign corporates. It is seen by some as a response to the U.S. legal and regulatory authorities having subjected scores of large French corporates and financial institutions to U.S. extraterritorial action (BNP Paribas, Technip, Société Générale, Alstom etc.).

Seven economic sectors considered to be at high risk of corrupt practices by the OECD are listed in the Circulaire Belloubet. The PNF is thus encouraged to monitor closely these sectors, specifically: construction, mining, transportation, telecommunications, pharmaceuticals, energy and military equipment. The PNF recently opened an investigation against a large French energy company concerning alleged acts of corruption in the sale of uranium in Nigeria.

Cross-border coordinated enforcement activity

French enforcement authorities are keen to collaborate for cross-border investigations.

The French Anti-Corruption Agency (AFA) stated in its 2020 guidelines that cross-border cooperation is a priority.

A 2020 CJIP was a milestone in terms of international collaboration of white collar enforcement activity. In the aerospace CJIP (referred to above), the PNF collaborated with the UK Serious Fraud Office (SFO), and the U.S. Department of Justice (DOJ) and State Department to reach a coordinated settlement in which the company agreed to pay EUR3.6bn for alleged corrupt practices. The PNF and the SFO had signed a cooperation agreement and worked together as part of a joint investigation team to conduct the investigation.

The French/U.S./UK collaboration in this matter revitalised the French Blocking Statute. This prohibits the transfer of information abroad in the context of, or with a view to, foreign judicial or administrative proceedings, outside the relevant international cooperation channels (ie the Hague Convention, MLATs, MOUs between agencies). The PNF relied on the Statute to control the flow of information to the UK and U.S. authorities. This assisted the PNF in taking the lead on the investigation.

The report drawn up by an MP in June 2019, at the request of the French Prime Minister, recommending increased penalties for violations of the Blocking Statute has not yet led to any action.

A coordinated settlement is beneficial for a company facing investigations in more than one jurisdiction, in order to avoid the risk of double jeopardy. In May 2020 the Paris Court of Appeal fined a telecom company for actively bribing foreign officials. Although a settlement agreement had been signed with a foreign enforcement authority, the Court of Appeal refused to apply the non bis in idem principle (which protects criminal defendants against double jeopardy) as some of the fraudulent behaviour had occurred in France and was not therefore covered by the settlement.
Financial crime issue predictions for 2021

The European Public prosecutor is set to become operational in 2021, an authority empowered to prosecute criminal offences “affecting the financial interests” of the EU, such as fraudulent or corrupt behaviour affecting its budget through, for example, the misappropriation or misuse of European subsidies. This independent prosecuting corps promises to investigate cases that Member States did not have the means to prosecute, or did not prioritise, in particular due to difficulties intrinsic to cross-border collaborations which are often resource-intensive.

Reports\(^5\) indicate that huge amounts of subsidies are misappropriated or misused each year, and that nearly EUR60bn is lost yearly to cross-border VAT fraud alone.

The European public prosecutor has indicated that it had received up to 3,000 cases from Member States that may fall under its jurisdiction. European white collar litigation promises to be one of the important features of 2021, as Member States increase collaboration in prosecuting such cases.

The increasing level of fines and penalties incurred by financial institutions, particularly in respect to tax evasion and tax fraud, serves as a reminder that the French financial and banking industry are also still being particularly targeted by enforcement authorities.

“A very dynamic, highly responsive and available team. The firm provides practical advice and good insight in the actual functioning of the different French authorities.”

2020, Legal 500 EMEA: France – Dispute resolution: White collar crime

“The firm has a leading banking criminal regulatory expertise.”

2020, Legal 500 EMEA: France – Dispute resolution: White collar crime

“Allen & Overy LLP handles a high volume of criminal tax-related matters including several headline cases, defending leading banks, companies and their corporate officers.”

2020, Legal 500 EMEA: France – Dispute resolution: White collar crime

“Well-reputed practice with an extensive international network and notable cross-border strength. Especially recognised for its activity in the financial institution space.”

2020, Chambers & Partners Europe: France – Litigation

\(^5\) European Court of Auditors special report – Fighting fraud in EU spending : action needed, 2019
“Denis Chemla has notable expertise in financial and commercial disputes. He represents domestic and international corporates as well as banking clients.”
2020, Chambers & Partners Europe: France – Litigation

“The distinguished Denis Chemla is adept at handling white collar crime and regulatory defence proceedings for large corporates. Denis Chemla has an ‘impeccable reputation in product liability work’ and a strong background in aviation matters.”
2020, Who’s Who Legal: France

“Hippolyte Marquetty is extremely skilled, responsive and practical. He perfectly understands his clients’ goals and knows how to put together a well-adapted and perfectly suited strategy.”
2020, Legal 500 EMEA: France – Dispute resolution: White collar crime

“Dan Benguigui has strong criminal banking regulatory expertise.”
2020, Legal 500 EMEA: France – Dispute resolution: White collar crime

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  
Counsel – 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 Associea – 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
Germany

The criminal enforcement environment in Germany remains robust. Criminal investigations into cum/ex trades are being pursued with high intensity. After the first criminal trial on cum/ex trades ended with convictions of the two defendants and a confiscation against a German bank in March 2020, new trials are currently being prepared or have already started. Besides this, the Wirecard scandal shocked Germany in June 2020 and resulted in criminal allegations and investigations. Furthermore, criminal investigations into the diesel emissions scandal are still affecting many car manufacturers and car components suppliers.

A revised draft bill of a German Corporate Sanctions Act is currently being negotiated in the German Federal Parliament (Bundestag). The Corporate Sanctions Act, expected to be passed by September 2021, will introduce a new system of sanctions for corporate crimes and will impact the conduct of internal investigations.

German authorities are also focusing on the prevention of money laundering and terrorist financing. In line with European legislation, this has led to stricter regulations under the German Money Laundering Act and a draft bill to significantly expand the scope of application of the money laundering offence in the German Criminal Code.

Investigations trends/developments

Enforcement actions by German criminal prosecution authorities relating to cum/ex trades, including potential dawn-raids, will continue in 2021. The Cologne Public Prosecutor’s Office is now conducting criminal investigation proceedings into cum/ex trades against more than 900 suspected individuals.

The German Federal Office of Administration (Bundesverwaltungsamt) has begun to more closely monitor compliance with reporting obligations to the transparency register under the German Money Laundering Act.

The authority imposed several corporate administrative fines due to violations of these obligations and more are expected. The enforcement decisions taken by the German Federal Office of Administration have been made publicly available on the authority’s website.
Significant law reforms impacting corporate criminal liability

A new law on corporate criminal liability is expected to be passed soon. The German Federal Parliament (*Bundestag*) is discussing the latest draft bill of the German Corporate Sanctions Act. Some provisions have changed since the original draft bill was proposed by the German government in August 2019. For example, corporate fines against companies that cooperate with the authorities and conduct an internal investigation “shall” (instead of “can”) be reduced by up to 50%. The option to dissolve a company as a consequence of corporate crime has been removed. We expect the Corporate Sanctions Act to be passed before September 2021. Read more.

To combat money laundering and terrorist financing, an amended and considerably stricter Money Laundering Act came into force in 2020 in line with European legislation. The new law stipulates, inter alia, enhanced due diligence requirements in high risk cases and facilitates public access to the transparency register. The Federal Government prepared a draft bill to improve the criminal law framework for combating money laundering and to implement Directive (EU) 2018/1673 (6MLD). This draft law widens the scope of the money laundering offence in section 261 of the German Criminal Code by abandoning the list of predicate offences and instead taking an ‘all crimes’ approach. This means that any offence from which property has been obtained will suffice as a predicate offence.

On tax evasion, the parliamentary groups of the governing parties in the *Bundestag* agreed to extend the existing limitation period for serious tax evasion from 10 to 15 years. The *Bundestag* and the German Federal Council (*Bundesrat*) approved the relevant law before year-end. This is seen as a measure to prevent certain cum/ex trading related offences from becoming time-barred.

Internal investigations – key developments

The German Corporate Sanctions Act will introduce a set of rules for the conduct of internal investigations. A notable change since the original draft bill of August 2019 is that the amended draft bill prompts a court to reduce the statutory maximum fine if a company has conducted an internal investigation and cooperated fully with the authorities. The court must take into account the range of facts revealed by an internal investigation, their importance for the authorities’ investigation and the timing of disclosure. Another notable change is the removal of the option for a court to reduce a fine if a company discloses the results of the internal investigation after court proceedings have begun. This is designed to encourage early cooperation.

The provisions on employees’ rights during an internal investigation have not changed. Companies must still consider the General Data Protection Regulation when reviewing personal data during internal investigations.

On a separate note, the German Corporate Sanctions Act will most likely not enhance the very limited protection of documents prepared in the context of an internal investigation from seizure by German criminal prosecution authorities.
Sectors targeted by law reforms or enforcement action

Due to the ongoing Wirecard scandal in Germany, an action plan, which had been developed by the Federal Ministry of Finance and the Federal Ministry of Justice and Consumer Protection, was presented to the Federal Cabinet in October 2020. The action plan aims at fighting accounting fraud and strengthening control over capital and financial markets. The Federal Financial Supervisory Authority’s (BaFin) powers are to be expanded. Among other things, BaFin will enjoy additional audit rights and rights to information in relation to capital market-oriented companies.

In connection with the Wirecard scandal, German prosecution authorities launched several criminal investigations and arrested the former Wirecard CEO as well as other Wirecard managers. Wirecard’s former COO is now a fugitive and his name is on Interpol’s most wanted list.

The investigations into the diesel emissions scandal are still impacting many car manufacturers and car components suppliers in Germany. A former Audi CEO became the first top executive to stand trial for his role in the diesel emissions scandal in September 2020. According to the criminal court’s provisional schedule, the trial is expected to continue until the end of the year 2022.

Most national and international banks are affected by cum/ex enforcement action. The Cologne public prosecutor’s office conducted a dawn raid in the context of cum/ex trades at the German Association of Banks (Bundesverband deutscher Banken e.V.). The Regional Court of Bonn was the first German court to decide that the participants in cum/ex trades may be held criminally liable – two former London bankers were found guilty of tax evasion in particularly severe cases. Due to the defendants’ cooperation with the prosecutors, their prison sentences were suspended. The next criminal trial at the Regional Court of Bonn, this time against a defendant with a more aggressive defence strategy, began in November 2020. The Regional Court of Wiesbaden has issued an arrest warrant for a well-known German lawyer residing in Switzerland who is alleged of having played a key role in setting up cum/ex schemes.

Cross-border coordinated enforcement activity

German authorities continue to reach out to foreign authorities in mutual legal assistance procedures in cross border matters. There are also indications that German criminal prosecution authorities share information and align enforcement activities with other European criminal prosecution authorities in relation to cum/ex trades which are said to have occurred in a number of jurisdictions.

Financial crime issue predictions for 2020

In house legal and investigations teams will need to familiarise themselves with the regulations set out in the draft Corporate Sanctions Act, as it is very likely that the draft bill will be enacted in 2021. In addition, we expect to see an increasing number of further investigations into allegations of money laundering and violations of the reporting obligations to the transparency register under the German Money Laundering Act.
“The compliance practice is well connected in the financial sector.”
JUVE handbook 2020/2021

“[Jan Erik Windthorst] provides smart and clear legal advice.”
JUVE handbook 2020/2021

“[Wolf Bussian] is good at handling disputes on tax-driven transactions.”
JUVE handbook 2020/2021

“Wolf Bussian and Jan Erik Windthorst both have strong expertise in internal investigations in the financial sector.”
Legal 500 Germany 2020

“Another focus of the practice are tax investigations.”
Legal 500 Germany 2020

“Tim Nikolas Müller enriches the team with expertise in white collar crime and sanctions-related advice.”
Legal 500 Germany 2020

“Tim Nikolas Müller – key lawyer for internal investigations.”
Legal 500 Germany 2020

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 5658  
laura.jung@allenovery.com

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

Hong Kong saw the enactment of the National Security Law (NSL) in 2020. Corporations or financial institutions are likely to be carrying out detailed and ongoing internal analysis to ensure their businesses are NSL compliant from different perspectives, including anti-money laundering and data protection. Although financial regulatory enforcement actions remain relatively quiet during the Covid-19 pandemic, Hong Kong financial regulators continue to focus on “high-impact” cases and senior management accountability, and thematic reviews to ensure proper market standards are met. The Hong Kong Monetary Authority (HKMA) is expected to implement a mandatory reference checking scheme to address the “rolling bad apples” phenomenon. On the anti-corruption front, the Court of Final Appeal handed down a judgment in line with the modern anti-corruption legislation in challenging secret payments received by agents. Appellate guidance in an uncertain area of law concerning cyber fraud is expected soon.

Investigations trends/developments

The Securities and Futures Commission’s (SFC) enforcement actions remain relatively quiet compared to 2019. The enforcement actions statistics for Q3 2020 (presented by way of a year on year comparison) published by the SFC are consistent with that general trend:

- A 28.3% decrease in the number of directions seeking information regarding offences including market misconduct, fraud, misfeasance and disciplinary misconduct.

- A 28.6% decrease in the number of investigations started by the SFC, and a 27.8% increase in the number of investigations completed by the SFC.

- A 23.5% decrease in the number of notices of proposed disciplinary action.

The Covid-19 pandemic will undoubtedly have had an impact on the SFC’s activity in 2020. The SFC continues to focus on “high-impact” cases and adopts a targeted approach to enforcement.

For example, the SFC imposed a fine of HKD400m on a financial institution for serious internal control deficiencies, which led to it overcharging its clients through post-trade spread increases and excess charges over a ten-year period. In October 2020, the SFC fined a financial institution HKD2.71bn (the largest amount fined by the SFC) for, inter alia, internal control failures relating to the 1MDB scandal.

Internal control deficiencies are still very much on the SFC’s radar. It imposed HKD78.1m in fines on companies for internal control deficiencies in 2020. The SFC has also reminded licensed and registered persons to remain focused on internal controls to ensure financial and operational resilience during the pandemic.
The SFC’s focus on senior management accountability remains clear. The SFC banned a former responsible officer (RO) from re-entering the industry for 12 months, as the RO’s conduct fell short of the standard required. The HKMA’s Consultation Paper on the Implementation of the Mandatory Reference Checking Scheme to Address the “Rolling Bad Apples” Phenomenon reinforces the importance that regulators place on conduct, culture and governance in Hong Kong.

See the following publications for more analysis:
– SFC Enforcement Actions Trends and Tracker
– Regulatory focus on senior management accountability in Asia – a victim of Covid-19 coronavirus?

**Significant law reforms impacting corporate criminal liability**

Guidance on the proper approach to the status of “agent” under the Prevention of Bribery Ordinance (Cap 201) (POBO) section 9(1)(a) has been given by the Hong Kong Court of Final Appeal (CFA) in HKSAR v Chu Ang [2020] HKCFA 18. The provision provides that an agent who, without lawful authority or reasonable excuse, solicits or accepts any advantage as an inducement to or reward for any act in relation to its principal’s affairs or business shall be guilty of an offence. The CFA clarified that no pre-existing legal relationship is required for one to be an “agent” of another under section 9. It need not even be proved that that other person had requested the agent to act. A person is an “agent” simply by having “acted for another” where that person has agreed or chosen so to act in circumstances giving rise to a reasonable expectation, and hence a duty, to act honestly and in the interests of that other person to the exclusion of its own interests.

The judgment is in line with the wide net cast by modern anti-corruption legislation in challenging secret payments made and received by those acting on behalf of another. Agents are certainly in the firing line, whether acting in a formalised arrangement or in a one-off transaction.

When an entity acts for another (no matter what the relationship is), it should remain honest and act in good faith and should not place itself in a situation of conflict of interest that would subvert the integrity of the relationship.

**Internal investigations – key developments**

In January 2020, the Privacy Commissioner for Personal Data (PCPD) identified a number of areas of reform to enhance and strengthen the Hong Kong personal data privacy regime, which are likely to impact how a corporate conducts internal investigations. These include:
– establishing a mandatory data breach notification mechanism;
– introducing a requirement to maintain a clear data retention policy;
– enhancing PCPD’s sanction powers;
– expanding Personal Data Privacy Ordinance’s (PDPO) reach to regulate data processors;
– amending the definition of personal data to cover information relating to an “identifiable” natural person; and
– prohibiting doxxing activities.

For example, a corporate will have to update its data retention policy to clarify how personal data gathered during an employee’s course of employment will be used in internal investigations, and how long the data will be retained.

In addition, if an employee is engaged in doxxing (ie non-consensual disclosure of an individual’s personal information for the purposes of harassment or intimidation) activities, the employer may have to consider conducting internal investigations and its reporting obligations.

We expect to soon see a draft bill. If enacted, these changes would create a more aggressive regulatory enforcement regime for data protection. See Hong Kong’s Privacy Commissioner for personal data – the end of the paper dragon.
Sectors targeted by law reforms or enforcement action

The SFC has increased its intervention in IPO applications. It received 303 listing applications (a 23.1% decrease from 394 in the previous year) via the Stock Exchange of Hong Kong. The SFC directly intervened in 35 initial public offering applications (a 106% increase from 17 in the previous year), using its regulatory powers under the Securities and Futures (Stock Market Listing) Rules. Intended IPO issuers should stay vigilant towards potentially serious disclosure or public interest issues.

Cross-border coordinated enforcement activity

The below graph illustrates that the enforcement-related requests for assistance received by the SFC (from overseas regulators) reached a peak in 2016/2017; the number since then decreased by 34% in 2019/2020. The enforcement-related requests made by the SFC (to overseas regulators) have decreased by 41% from 2015/2016 to 2019/2020.

Requests for regulatory cooperation

Nevertheless, even though the requests for regulatory cooperation between the SFC and overseas regulators are on a downward trend, licensed corporations should note that breach of foreign law may cause the SFC to be concerned over their fitness and properness. For example, the SFC recently reprimanded and fined a licensed corporation HKD1.5m for failing to ensure compliance with applicable laws and regulations in distributing investment funds and offering investment advice in Taiwan and failing to adequately supervise the business activities of its representatives to ensure such compliance.

In addition, during Q3 2020, the China Securities Regulatory Commission (CSRC) provided investigatory assistance for several of the SFC’s cases, despite travel restrictions amidst the Covid-19 pandemic. The SFC also held in-depth discussions on high-priority cases with the CSRC.

Licensed corporations should remain vigilant when carrying out overseas business.

---

Financial crime issue predictions for 2020

National Security Law

GCs and in-house legal teams will likely remain focused on the NSL, the need to ensure compliance, and the risk of being brought within an investigation of third parties alleged to have committed an offence. A number of issues may be of concern:

First, an authorised institution (AI) in Hong Kong should file a suspicious transaction report (STR) under the NSL as soon as reasonably practicable when it “knows” or “suspects” that any property/proceeds is related to an offence under the NSL.

Secondly, new enforcement powers have been given under the NSL. For instance, police officers designated by the Secretary for Justice have power to order removal of electronic messages endangering national security and disclosure of identification record or decryption assistance. This is particularly relevant to platform, hosting and network service providers which host data and control access to electronic messages.

In addition, for the purpose of assisting an investigation into an offence endangering national security or the proceeds obtained with the commission of the relevant offence, either the Secretary for Justice or designated police officers may apply to the court for an order to require a person that has the required information to answer questions within a specified time period, or to furnish or produce the relevant information or material.

It will be of commercial importance to minimise the risk of being caught within an investigation of third parties and thereby prevent normal operations from being disrupted by the exercise of such enforcement powers.

Cyber fraud

There has been a significant increase in cyber fraud cases since the Covid-19 outbreak. Cyber-attacks are increasing in frequency and sophistication, both globally and within the Asia-Pacific region. Banking and financial institutions are prime targets for such attacks.

In addition, Hong Kong is one of the primary destinations for the proceeds of cyber fraud. It is estimated that 6.4 billion fake emails are sent globally every day, resulting in USD26bn of global losses, according to the FBI’s international statistics for reported cases. A large financial media corporation lost USD29m in an alleged email fraud involving international transfers of money from its U.S. subsidiary to Hong Kong recipients. On the back of this fraud, the corporation has obtained injunctive relief against certain defendants in the Hong Kong court.

As a result, we expect an increase in civil recovery actions before the Hong Kong courts, and regulatory enforcement action in cyber security is expected to increase.

As for the former, it is important for victims to take actions swiftly after discovering a fraud to increase the prospect of recovery of the misappropriated funds. We have created the Hong Kong Cyber Fraud First Response Tool, which guides the victims of cyber fraud through the immediate steps they should take following the discovery of a fraud.

There have been a number of court proceedings commenced by victims of cyber fraud. In addition to declaratory relief, default judgment and injunction, the plaintiffs (victims) often apply for a vesting order (compelling the bank to transfer the money in the recipient’s account to the victim) under the Trustee Ordinance (Cap. 29) against the recipients of the funds. These applications have given rise to a number of recent divergent decisions as to whether a constructive trust can arise and vesting orders be granted under the statute. While there is likely to be more court decisions on this topic, we expect there will be appellate guidance in this uncertain area of the law.

The SFC has reminded licensed corporations to assess their operational capabilities and implement appropriate measures to manage the cyber security risks associated with their remote working arrangements. Corporations should also consider updating employee training materials on remote IT security.

---


Allen & Overy “offers a strong contentious offering, including handling high-profile investigations”.
Chambers Asia Pacific 2020, Financial Services (International Firms), China

“Offers expertise in regulatory investigations and mis-selling claims, leveraging off the strength of the firm’s fraud, white collar crime and money-laundering practices.”
Chambers Asia Pacific 2020, Dispute Resolution: Litigation (International Firms), China

Fai Hung Cheung “advises clients on a wide range of white collar crime, shareholder disputes, debt recovery and banking litigation mandates”.
Chambers Asia Pacific 2020, Dispute Resolution: Litigation (International Firms), China

Matt Bower “rises in the rankings after receiving significant praise for his commercial and financial litigation practice, which spans contentious regulatory issues and shareholder disputes”.
Chambers Asia Pacific 2020, Dispute Resolution: Litigation (International Firms), China

Key team members

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

Fai Hung Cheung
Partner – Hong Kong
Tel +852 2974 7207
fai.hung.cheung@allenandover.com
Despite Covid-19, there was no stagnation in the investigation and prosecution of white collar crime in the Netherlands. The Dutch regulators and the Dutch Public Prosecution Service (DPPS) remained focused on the fight against money laundering and corruption. A collective transaction monitoring entity was established by five Dutch Banks to jointly monitor payment transactions for signals that may indicate money laundering. For large Dutch out-of-court settlements, a policy reform entered into force which introduces an assessment by an independent review committee.

The Netherlands remains an active jurisdiction for cross-border white collar crime and investigations in 2020 and we expect this trend to continue in 2021.

**Investigations trends/developments**

The Dutch regulators and the DPPS continue to prioritise the fight against money laundering and corruption. The focus remains on AML compliance by gatekeepers such as banks, accountancy firms and notaries. For example, the DPPS is investigating ABN AMRO for alleged breaches of the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (the AML Act).

In a market-first, five Dutch banks (ABN AMRO, ING, Rabobank, Triodos and de Volksbank) joined forces in the fight against money laundering and established a collective transaction monitoring entity called Transaction Monitoring Netherlands (TMNL). TMNL will focus on identifying unusual patterns in payment traffic that individual banks cannot detect. The banks will jointly provide their payment data to TMNL, which will monitor the aggregated information for signals that may indicate money laundering.

A&O Amsterdam advised the banks on the foundation and establishment of TMNL in mid-2020. The first joint monitoring is expected to take place in 2021. Although TMNL is currently limited to the five banks, it is expected that other banks will be able to join in the future.
Significant law reforms impacting corporate criminal liability

In recent years, the amounts paid in Dutch out-of-court criminal settlements have increased significantly. Further to mounting criticism that these settlements lack transparency and judicial oversight, the Dutch government is working on a proposal for a judicial review mechanism for large criminal settlements. In anticipation of this judicial review, a policy reform entered into force in September 2020 which introduces an assessment of out-of-court criminal settlements with a fine of EUR200,000 or a total amount of EUR1m or more by an independent review committee. This review committee consists of a former white collar defence lawyer, a former criminal judge, a professor of criminal (procedure) law and two former public prosecutors. Three appointed members of this committee will assess whether the settlement proposal is appropriate and reasonable. For this assessment, the committee will consider a draft settlement agreement, a statement of facts and a draft press release, and will organise two hearings behind closed doors to allow the DPPS and the suspect and its counsel to present their views on the proposed settlement. The review committee is expected to review its first settlement proposal in 2021.

The DPPS published a revised version of its Instruction regarding the Investigation and Prosecution of Foreign Corruption (Instruction) in October 2020. The Instruction and its predecessors give a useful insight into the priorities of the DPPS regarding prosecuting bribery and corruption. The previous version of the Instruction stated that the DPPS would not, in certain circumstances, prosecute facilitation payments. The revised version of the Instruction does not include this statement. Although the DPPS did not provide any explanation for this alteration in the Instruction, it could mark a stricter approach being taken by the DPPS to facilitation payments.

Internal investigations – key developments

As in previous years, there is public debate in the Netherlands regarding the scope of legal privilege in corporate investigations. A connected development is the release of a draft bill for consultation that proposes limiting the scope of legal privilege in tax matters. This draft bill proposes that the legal privilege of lawyers only covers information that is directly linked to lawyers’ activities for the determination of the legal position, representation and defence of their clients and advice before, during and after legal proceedings. This would, for example, mean that communications regarding tax advice or other legal 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.

In June 2020, the DPPS announced that it wishes to increase cooperation with lawyers retained by a suspected company to conduct an internal investigation. The DPPS recognises the benefit of such cooperation, in that it reduces pressure on the authorities. The current Dutch legal framework lacks concrete guidelines regarding sentencing leniency after self-investigation and self-reporting. However, recent developments suggest that such action by a suspected company may be taken into account when a settlement amount is determined. This announcement by the DPPS sparked debate in the Netherlands as to whether lawyers routinely retained by a company should be involved in an internal investigation. Some say that a company’s external lawyers may lack independence, while others believe that independence is not an issue, and emphasise the practical benefits of this cooperation. We expect this debate to continue in 2021.
Sectors targeted by law reforms or enforcement action

The Dutch regulatory authorities and the DPPS remained focused on compliance with AML and corruption regulations by the financial services sector, including financial institutions, payment service providers and accountancy firms. Specifically, the authorities paid more attention in 2020 to the quality and future resilience of financial institutions’ data management in relation to AML. This is partly due to the fact that financial institutions are seeking more access to personal financial data in order to comply with AML regulations.

There was also more emphasis on cyber security in response to the increase of complex cybercrime offences. As almost all sectors are susceptible to cybercrime, the Dutch government is putting more emphasis on the awareness of the duty of care incumbent on companies to monitor cyber security risks and take mitigating measures. The Dutch Minister of Justice and Security recently criticised the lack of effectiveness of enforcement in this regard, and expressed an aim to, inter alia, start a legislative procedure to oblige all vital service providers under the Cyber Security Act, such as banks, to meet a minimum digital security level.

Cross-border coordinated enforcement activity

In recent years, the Netherlands has actively worked to increase its cooperation with foreign investigative and prosecutorial agencies. Since mid-2018, it has been 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.

The J5 Group noted a number of successes in 2020, including a globally coordinated “day of action” in relation to a suspected offshore tax evasion scheme. The action was part of an investigation which started with information obtained by the Dutch tax authority.

The J5 Group started using the electronic platform Financial Criminal Investigation (FCInet) for its information sharing. This is a decentralised virtual network that enables the J5 members to compare, analyse and exchange data anonymously.

The Netherlands is also one of the participating states in the European Public Prosecutor’s Office (EPPO). The Dutch public prosecutor Daniëlle Goudriaan was appointed as one of the European Prosecutors of the EPPO, which is expected to become operational in early 2021 and is intended to combat various forms of fraud, money laundering and corruption.

Financial crime issue predictions for 2020

The impact of Covid-19 on the investigation capacity of the DPPS and Dutch regulators has been limited, since the majority of prosecutors and investigators were able to continue their work from home. The only type of investigative activity that has been postponed since March 2020 is the execution of dawn raids. On this basis, it is likely that the external kick-off of a number major investigations has been postponed, and therefore likely that the lifting of Covid-19 related restrictions will bring to light a number of pending investigations.

There has been a shift of focus with regard to the enforcement of international sanctions. Investigative and prosecutorial capacity has been increased and we have seen the enforcement focus shift from flagrant offences by individuals and small companies to large international companies that may not have effective compliance programmes.
Allen & Overy LLP’s team is described as “absolutely good in investigations, the lawyers understand the way to handle them”.

Chambers Europe: White collar Crime & Corporate Investigations

Hendrik Jan Biemond is described as “one of the best lawyers on the criminal side in the Netherlands”.

Chambers Europe: Dispute Resolution – White collar Crime – 2020

Neyah van der Aa is described as “impressive” and “hands-on”.

Chambers Europe: Corporate Investigations – 2020

Key team members

<table>
<thead>
<tr>
<th>Name</th>
<th>Position – Location</th>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neyah van der Aa</td>
<td>Senior Associate – Netherlands Tel +31 653 889 291 <a href="mailto:neyah.vanderaa@allenovery.com">neyah.vanderaa@allenovery.com</a></td>
<td></td>
</tr>
<tr>
<td>Fleur le Roy</td>
<td>Associate – Netherlands Tel +31 682 359 843 <a href="mailto:fleur.leroy@allenovery.com">fleur.leroy@allenovery.com</a></td>
<td></td>
</tr>
<tr>
<td>Micha Boucher</td>
<td>Associate – Netherlands Tel +31 682 753 241 <a href="mailto:micha.boucher@allenovery.com">micha.boucher@allenovery.com</a></td>
<td></td>
</tr>
</tbody>
</table>
South Africa

The judicial commissions of inquiry into allegations of corruption and other forms of white collar crime have dominated the South African media cycle. The State Capture scandal remained a key issue in South Africa in 2020, with a number of enforcement actions commencing in 2020. At the same time, the Covid-19 pandemic has seen a wave of new corruption allegations, particularly regarding the procurement of personal protective equipment. In 2021, we expect to see further prosecutions and enforcement action, as well as civil recovery action in respect of misappropriated public funds.

Investigations trends/developments

**Bribery and corruption:**
In the context of the State Capture scandal, the South African government declared that it would prioritise increased enforcement against white collar crime and the recovery of funds misappropriated from state coffers.

Over the course of 2020, a number of persons implicated in State Capture were arrested and charged. In addition, Eskom, the state power utility, along with the Special Investigations Unit have instituted civil action against a number of individuals for the recovery of approximately ZAR3.8bn allegedly siphoned from the power utility through dubious means. Further arrests, prosecutions and civil recovery actions are expected in 2021.

**Anti-Money Laundering:**
The Prudential Authority concluded its first Anti-Money Laundering and Combating the Financing of Terrorism risk assessment within the banking and life insurance sectors.

The Prudential Authority’s assessment rates the banking sector as representing a medium-to-high risk and notes a number of vulnerabilities in the sector’s ability to monitor and address money laundering and terrorism financing risk, including:

- the use of cryptocurrencies, specifically persons using the system to convert digital currency to legal tender, and susceptibility to cybercrime;
- poor functioning of systems, which limits the ability of a bank to have a single-client view, and systems which do not enable continuity and stability;
- a lack of automated controls to address money laundering and terrorist financing risks;
- products and services offered which are linked to a cash-based economy;
- difficulties in obtaining beneficial ownership information and identifying the source of funds;
- inadequate information-sharing between financial institutions; and
- incorrect risk profiling of persons.

The Prudential Authority’s assessment rates the life insurance sector as a medium risk due to the absence of mitigating controls to address the following deficiencies, such as:

- inadequate processes to identify reportable cash transactions;
- inadequate management information systems for detecting patterns of unusual or suspicious activity, particularly in relation to higher-risk accounts;
- inadequate training of staff members responsible for reviewing customer transactions; and
- in some cases, lack of enhanced due diligence reviews and/or inadequacies in automated transaction monitoring.

We anticipate additional measures and/or guidance from the South African Prudential Authority to address these shortcomings in 2021. In addition, the Financial Action Task Force (FATF) will likely release an updated report following the mutual evaluation of the Anti-Money Laundering and Combating the Financing of Terrorism standards in South Africa.
**Significant law reforms impacting corporate criminal liability**

Significant amendments to the Prevention and Combating of Corrupt Activities Act have been in the pipeline for at least three years and were expected to be introduced in 2020. Unfortunately the reforms remain in draft form and have not yet been tabled before Parliament. We expect to see developments in this space in 2021.

In the interim, amendments have been proposed to the schedules to the Financial Intelligence Centre Act (**FICA**).

The proposed amendments include expanding the list of accountable institutions (who are subject to the obligations imposed by **FICA**) to include additional financial and non-financial businesses, including crypto asset services providers, and enabling the **FIC** to take over responsibility for oversight and enforcement of compliance with **FICA** in respect of the non-financial sector activities involving estate agents, gambling institutions, trust and company service providers and legal practitioners.

**Internal investigations – key developments**

The long-awaited Protection of Personal Information Act (**POPIA**) commenced on 1 July 2020 and gave effect to the constitutional right to privacy and provided a framework for the lawful processing of personal information in South Africa. **POPIA** is modelled largely on the predecessor of the General Data Protection Regulation, EU Directive 95/46/EC, however a key difference is that **POPIA** also applies to the processing of personal information of juristic persons. Responsible parties (controllers) are afforded a 12-month grace period to ensure compliance; therefore, enforcement of the protections contained in **POPIA** will commence on 1 July 2021. In-house legal and investigations teams would be well advised to review internal compliance programmes and ensure that personal information is processed in accordance with **POPIA**.

In March 2020, the Financial Intelligence Centre (**FIC**) finalised the Public Compliance Communication to provide guidance in respect of the usage of an Automated Transaction Monitoring Systems. Furthermore, in November 2020, the **FIC** published a draft Public Compliance Communication to elaborate on how to review a particular geographic area as an indicator to assist in the formation and application of the risk-based approach to money laundering, terrorist financing and proliferation financing. Public Compliance Communications constitute authoritative guidance and set out the **FIC**’s view on a particular issue and the practical application of **FICA**. Corporates should therefore familiarise themselves with these documents to ensure compliance with **FICA** obligations.

**Sectors targeted by law reforms or enforcement action**

The State Capture commission’s focus continues to be on the IT, accounting and consulting sectors.

However, the financial sector has increasingly become an area of focus and we expect this sector to be a key focus for 2021.
**Cross-border coordinated enforcement activity**

Despite South Africa being party to a number of mutual legal assistance treaties and cross-border cooperation agreements, there has been no new significant cross-border enforcement activity this year. The antitrust regulator continues its enforcement action against global banking institutions pursuant to allegations of currency manipulation.

In the second half of 2020, South Africa announced that it will be investing in border security by introducing new border management legislation and establishing a border management authority. The efficacy of these measures in preventing illegal immigration and human trafficking and providing for enhanced regulation of goods moving across borders remains to be seen.

**Financial crime issue predictions for 2020**

We expect to see an increased focus on data protection. The term of office in respect of the current members appointed to the Information Regulator will terminate in December 2021, therefore we would not be surprised to see a flurry of enforcement activity between July and December 2021.

In addition, the fallout from the State Capture inquiry will continue to be a concern for entities that conduct business with the South African government, as will white collar crime emanating from the private sector. With regard to the latter, the Johannesburg Securities Exchange has levied a ZAR13.5m fine against Steinhoff International for failing to comply with listing requirements and has noted that its investigations into individuals at the company are ongoing. We anticipate additional fines, increased civil recovery action and criminal prosecution activity.

**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

**Siphosethu Khumalo**  
Candidate Attorney – Johannesburg  
Tel +27 10 597 9884  
siphosethu.khumalo@allenovery.com
The UAE’s approach to white collar crime has come under particular scrutiny over the past year following scheduled reviews by international organisations and a number of high profile cases involving UAE companies.

The UAE has continued to develop and bolster its efforts to tackle white collar crime, both within its “onshore” jurisdictions and within the various “offshore” free zones, most prominently the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM), which are subject to the same criminal law but which have their own compliance and regulatory regimes.

Recent legislation has expanded the remit of local regulators beyond financial institutions to cover other high risk sectors of the UAE economy. This has been the case for both onshore regulators (such as the UAE Central Bank) and offshore regulators, such as the DIFC’s Dubai Financial Services Authority (DFSA) and the ADGM’s Financial Services Regulatory Authority (FSRA).

The implementation and enforcement of this new legislative framework is likely to be a major policy focus for the UAE in the coming years.

Investigations trends/developments

**Financial Action Task Force – Mutual Evaluation Report**

The trends expected to dominate the coming year are likely to be influenced by the contents of the Financial Action Task Force (FATF)’s [UAE Mutual Evaluation Report (MER)](https://www.fatf-gafi.org/) of April 2020. The MER measures a country’s adherence to anti-money laundering (AML) best practice and serves as a critical barometer of security and sophistication in combatting financial crime.

**UAE’s progress**

The MER highlighted the significant improvements made by the UAE since FATF last assessed its AML framework in 2008, including:

– the development of a National Risk Assessment of the money laundering threats faced by the UAE;

– sweeping technical reform in legislation and regulation, notably through Federal Decree No. 20 of 2018 (the AML Law);

– strengthening coordination mechanisms across the Emirates; and

– strengthening the Central Bank’s Financial Intelligence Unit.

The UAE also received praise for its effectiveness in prosecuting instances of terrorist financing.
These measures are significant given the unique challenges faced by the UAE: its proximity to conflict zones and sanctioned regimes, its low-tax economic model and the high remittance rate among its population (88% of whom are foreign nationals). The UAE’s achievements in this regard are underscored by its favourable ranking in Transparency International’s most recent Corruption Perceptions Index, in which the UAE overtook both France and the United States.

Policy goals

The MER identified several areas where further work is needed, including the following:

a. improve the effectiveness of controls (at the regulatory and the firm level) for preventing money laundering activity;
b. refine the understanding of money laundering risks, particularly regarding the deployment of professional money laundering networks;
c. enhance money laundering investigations and prosecutions;
d. centralise information related to ultimate beneficial ownership.
e. formalise the approach to international cooperation; and
f. better supervise industries outside the financial sector which are connected to money laundering activity.

Steps in achieving the MER goals

The above areas are likely to be the focus of the UAE’s efforts to combat money laundering over the coming years. The legislative framework for meeting these goals is already largely in place.

There are likely to be increasing enforcement efforts, with a wider range of sanctions for non-compliant entities. Enforcement is unlikely to be limited to financial institutions as the most obvious targets: the authorities are likely to target Designated Non-Financial Businesses and Professions (DNFBPs).

Significant law reforms impacting corporate criminal liability

The AML Law

The AML Law remains the centrepiece of the UAE’s legislative framework in combatting financial crime, having introduced:

– a “controlled delivery” operation: whereby the UAE authorities may permit a criminal transaction to proceed in order to trace the flow of money;

– the concepts of:
  i. “predicate offence” defined as “any act constituting a felony or misdemeanour under applicable laws of the UAE; whether the act is committed inside or outside of the UAE”; and
  ii. “perpetrator” which includes any person “gaining” or “possessing” illegal proceeds: a perpetrator’s offence under the AML Law is independent of the predicate offence;

– AML and CFT customer due diligence and other compliance obligations incumbent on DNFBPs;

– powers for the UAE Public Prosecutor to compel disclosure from a range of third parties and for the UAE Central Bank to freeze funds deposited at UAE financial institutions;

– an increased cap of AED50m for corporate liability for money laundering offences; and

– compulsory liquidation where an illegal activity is related to terrorist financing.

Recent legislation

Recent legislative developments have focused on expanding and implementing the AML Law:

a. Federal Cabinet Resolution No. 10 of 2019 extended many of the AML Law’s provisions for financial institutions to cover the activities of DNFBPs;

b. Federal Cabinet Resolution No. 74 of 2019 introduced procedures and parameters for designating targeted entities or individuals, fleshing out practical elements of the AML Law;
c. Federal Cabinet Resolution No. 58 of 2020 introduced disclosure obligations regarding ultimate beneficial ownership;
d. Ministry of Justice Decision No. 533 of 2019 issued the AML-CFT procedures applicable to DNFBPs; and
e. Federal Law No. 14 of 2020 issued provisions regarding the protection of witnesses and whistle-blowers.

Circular of March 2020

The Circular issued by the UAE Ministry of the Economy in March 2020 (the Circular) clarified the interaction of the above legislation with the AML Law. As a result of this combined legislation, DNFBPs (as well as financial institutions) must:

a. comply with their reporting obligations to the authorities, with only very limited allowance made for any duty of professional confidentiality;
b. identify the crime risks within their scope of activity on a continuous basis;
c. implement any necessary procedures relating to customer due diligence (having considered the risk factors outlined in the National Risk Assessment);
d. refrain from conducting a commercial transaction under conditions of anonymity or on behalf of an alias;
e. promptly apply those directives of the competent authorities which implement the decisions issued by the UN Security Council (regarding terrorist financing); and
f. maintain all records relating to the above, and make these available to the competent authority on request.

Internal investigations – key developments

Expanded protection for whistle-blowers, both in onshore and offshore UAE jurisdictions, remains the major trend of which companies operating within the UAE should take note. The UAE authorities’ increased focus on whistle-blowing is evident both from new legislation and in the authorities’ efforts to make the process of whistle-blowing as accessible as possible, with simple, clear instructions prominently provided on regulator websites and with Abu Dhabi even having introduced an app to encourage whistle-blowing.

In the onshore UAE, at the federal level, explicit legal protection for whistle-blowers has been introduced under Federal Law No. 14 of 2020 (the Witness Protection Law). The Witness Protection Law provides for the establishment of a witness protection programme aimed at protecting victims, witnesses and whistle-blowers in crimes related to AML and CFT and cybercrime (among others).

In onshore Dubai, Article 19 of Law No. 4 of 2016 on Financial Crimes introduced immunity from both prosecution and disciplinary action for individuals who disclose to the Dubai Centre for Economic Security (an agency specifically created to monitor and reduce financial crime) information that is true and which relates to activity that may affect the economic security of Dubai.

Increased protections for whistle-blowers are also evident in offshore UAE jurisdictions. For example, the DIFC has introduced whistle-blower protections by virtue of DIFC Law No. 7 of 2018 (the Operating Law). Article 62 of the Operating Law creates a positive obligation to report wrongdoing while Article 64(3) protects those who in good faith disclose a possible contravention of the Operating Law by a DIFC entity from:

a. any legal or contractual liability for making the disclosure;
b. any contractual, civil or other remedy for making the disclosure; and
c. dismissal or victimisation from their place of employment.

The DIFC’s commitment to the Operating Law’s protections has been underlined by their incorporation into the DIFC’s employment code (DIFC Law No. 2 of 2019), but it is not yet clear how these protections will interact with UAE criminal law, particularly around areas such as confidentiality.
Sectors targeted by law reforms or enforcement action

Real estate

Real estate is identified throughout the MER as an area of particular concern from a money laundering perspective. A cash-driven sector, attractive to foreign investors seeking to store large sums, inevitably presents problems and is resulting in increased attention from the UAE authorities. This has been reflected by the inclusion of real estate brokers/agents as a DNFBP in Federal Cabinet Resolution No. 10 of 2019, bringing the sector within the purview of the AML Law.

Cyber-crime

The UAE authorities have signaled that cyber-crime will be an area of focus in the coming years. On 24 June 2020, the DFSA published a report, the Cyber Thematic Review, on the cyber risks faced by firms providing financial services in the DIFC. The report noted the increased frequency and severity of cyber-attacks and raised several concerns as to the resilience of DIFC firms, highlighting a lack of engagement at the board level and the limited use of cyber intelligence platforms by small and medium sized firms.

This focus is crystallising into tangible measures, most notably with the establishment of the DFSA Cyber Threat Intelligence Platform (TIP) in January 2020, which is available to all DIFC companies and which serves as a platform for the quick sharing of information on current cyber-threats between those entities and the DFSA as regulator. The TIP is the first such regulator-led intelligence platform in the Middle East and draws upon the cyber-security expertise of both the public and private sectors, with contributors to its operation including the Dubai Electronic Security Centre and Kaspersky Laboratories.

Cross-border coordinated enforcement activity

Formalised international coordination was highlighted by the MER as an area for development. Notably, the UAE’s growing status as a major international financial hub will necessitate coordinating with foreign authorities, particularly those of the United Kingdom and the United States.

While this will be a focus across the UAE’s offshore and onshore authorities, the offshore regulators in particular have recently expanded the scope of their international cooperation.

The DFSA has signed 109 bilateral and five multilateral memoranda of understanding with other regulators, with whom it frequently collaborates on cross-border matters: during the past year, the DFSA received 65 requests for regulatory information and assistance from other regulators, while the DFSA made 74 requests to fellow regulators for information.

Although the FSRA does not report statistics with regard to its international regulatory collaboration or enforcement action, it has now signed 115 regulatory memoranda of understanding with both national and international regulatory bodies (including international financial centres). Most notably, in November 2020 the FSRA agreed a memorandum of understanding with the Israel Securities Authority providing for regulatory cooperation.
Financial crime issue predictions for 2020

Adapting to the UAE’s new focus on AML measures
Pressure for businesses in the UAE, both onshore and offshore, to adapt to the changed legislative landscape is likely to mount throughout 2021 and greater formal and informal contact with regulatory bodies should be anticipated. DNFBPs in particular are likely to be subject to more stringent oversight, with a real threat of corrective action where they are in breach of their compliance obligations.

Commensurately, in-house legal teams should expect to devote more time to developing, updating and implementing compliance procedures, particularly in enhanced due diligence and suspicious transaction reporting. They will also need to defend the robustness of these procedures to internal and external stakeholders, each of whom are likely to be more attentive to AML issues.

Cyber-crime
Phishing attacks, impersonation of legitimate business partners and ransomware attacks are all likely to demand an increasing amount of attention from in-house IT and legal teams. The rapid growth in remote working during the Covid-19 pandemic has compounded the scope for such frauds, as highlighted in a recent FATF report. Collaboration between the UAE authorities and financial institutions to raise awareness of such frauds is likely to be a feature of 2021.
“Yacine Francis is described by clients as ‘very user-friendly, concise but also knows the big picture’. He is heavily involved in financial crime and fraud cases.”
Chambers Global 2019, Dispute Resolution, United Arab Emirates

“They have a really good team spirit in coordinating international cases across different jurisdictions, as well as understanding different legislations.”
Chambers Global 2020, Corporate Investigations, Global-wide

“They are incredibly responsive and their instincts as lawyers are so spot-on. Nothing is too much trouble and everything is done immediately to a very high level of quality. They are excellent and a joy to work with.”
Chambers Global 2020, Corporate Investigations, Global-wide

Key team members

<table>
<thead>
<tr>
<th>Yacine Francis</th>
<th>Ewa Kondracka</th>
<th>Thomas Abbasi</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Partner – Dubai</strong></td>
<td><strong>Associate – Dubai</strong></td>
<td><strong>Associate – Dubai</strong></td>
</tr>
<tr>
<td>Tel +971 4 426 7228</td>
<td>Tel +971 4 426 7291</td>
<td>Tel +971 4 426 7279</td>
</tr>
<tr>
<td><a href="mailto:yacine.francis@allenove.com">yacine.francis@allenove.com</a></td>
<td><a href="mailto:ewa.kondracka@allenove.com">ewa.kondracka@allenove.com</a></td>
<td><a href="mailto:thomas.abbasi@allenove.com">thomas.abbasi@allenove.com</a></td>
</tr>
</tbody>
</table>
United Kingdom

The UK has high ambitions to fight financial crime, though 2020 saw mixed success for enforcement authorities. While there were three more Deferred Prosecution Agreements (DPAs), including the first with a non-UK company relating to conduct abroad, there were some high-profile failures of corruption prosecutions against individuals whose employers had already entered into DPAs and paid fines, for the same alleged conduct.

A failed prosecution of a large international bank saw the UK’s rules on corporate attribution examined and reaffirmed, adding fuel to the fire for those seeking reform to make it easier to hold large companies criminally liable. Looking ahead, we expect to see proposals unveiled later this year for reform of corporate criminal liability. There will be increased financial crime risk and enforcement resulting from the perfect storm of market volatility, financial pressures and home working resulting from Covid-19 (eg market abuse, fraud, tax evasion offences). The pressure on UK companies to enter new (perhaps emerging) markets post-Brexit may mean a higher corruption risk.

Investigations trends/developments

**Don’t rush into a DPA:**
There have been no successful prosecutions of individuals following Deferred Prosecution Agreements (DPAs) and the corporate attribution rules mean that it can be difficult for prosecuting authorities to successfully prosecute corporate entities for criminal conduct. In 2020 some very high-profile post-DPA prosecutions by the SFO against individuals either collapsed or led to acquittal. This caused debate about whether the companies involved were wise to have entered into DPAs for conduct in which those individuals were alleged to have been involved. Did the weakness of the SFO’s cases against the individuals reveal inherent weaknesses in the case against the companies? Proponents of DPAs point to the benefits of finality and certainty rather than having a corporate prosecution hanging over a company for a number of years. Others question whether, given the continued difficulty that the SFO has suffered in successfully prosecuting large companies in criminal cases, companies should be rushing to enter into DPAs.

**Rules on corporate attribution examined and reaffirmed:**
The failed prosecution against a large bank has reinforced the narrow scope of corporate attribution in English law. The court decided that the conduct of the Chief Executive Officer and four senior individuals could not be attributed to the bank. The court reaffirmed the test for corporate attribution for crimes involving mens rea: the prosecutor must prove the guilt of the “directing mind and will” of the company. The ruling has added further fuel to the fire for those calling for reform of English law on corporate criminal liability.
Extraterritorial reach of UK Bribery Act 2010 confirmed:
Of interest to non-UK companies, the 2020 DPA with a global aerospace company, reached as part of a coordinated settlement with French and U.S. authorities, was the first, given the lack of UK conduct, to apply to a non-UK company through it ‘carrying on a business’ in the UK. The judgment did not examine the test in any detail, save that it found that the UK nexus (which was agreed as part of the DPA) was the Dutch parent company’s “strategic and operational management” of UK subsidiaries. This means that a non-UK parent company’s management of UK-incorporated subsidiaries may make the parent subject to the Bribery Act, even for conduct that is unrelated to the UK.

Access to documents held abroad:
Also of interest for non-UK companies, the UK Supreme Court heard the KBR v SFO appeal on the question of whether powers granted to the SFO to compel individuals or companies to produce evidence, have extraterritorial effect. This will determine whether the SFO has power to order KBR, a U.S. company, to produce documents held abroad in relation to the SFO’s investigation into a UK subsidiary. A 2018 Court of Appeal ruling in the case said that the SFO can compel production of documents held extraterritorially by a U.S. parent company, even where that parent company is not the focus of the UK investigation, if there is a “sufficient connection” between that company and a UK company under investigation. The outcome will impact the conduct of cross-border investigations. Read more.

Cross-border coordinated enforcement activity
Companies must assume that most authorities are speaking to their overseas counterparts, and plan accordingly. Continuing the trend of cross-border information sharing and coordinated investigations, the UK enforcement authorities continue to cooperate with 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.

In 2020 the SFO worked closely with the U.S. and French authorities to reach the world’s largest-ever bribery and corruption coordinated resolution, imposing a record-breaking EUR3.6bn fine on a global aerospace company. For this DPA, the SFO and PNF had worked as part of a Joint Investigations Team, which is an EU mechanism.

There has also been some cooperation at the legislative level. A new UK/U.S. bilateral agreement for accessing electronic data in cases of serious crime has entered into force in the UK. The agreement permits UK law enforcement agencies to apply to an English court to obtain electronic data directly from U.S. communication service providers, without the involvement of the U.S. authorities, a mutual legal assistance treaty or any of the other cumbersome routes currently used. There are tricky issues concerning the time frames for responding to such a request, confidentiality, privilege and data protection. The extent to which these orders will be enforceable in the U.S. also remains to be seen. Read more here.
Significant law reforms impacting corporate criminal liability

The scope of the UK’s money laundering regime was broadened in 2020 to include crypto asset exchange providers, custodian wallet providers, high-value art market participants (eg art dealers and freeport operators) and high-value property letting agents (where previously it was just estate agents). An expanded definition of ‘tax adviser’ means that those who offer material aid or assistance on tax matters also come within scope. The Money Laundering Regulations 2017 (MLRs) were also amended to allow law enforcement to request a wide range of account information from credit institutions to help them identify account holders and beneficial owners of funds. There are also non-substantive Brexit related changes to the UK’s AML laws to ensure that the regime works with the UK outside the EU.

A new autonomous UK sanctions regime came into force on 1 January 2021 as a result of Brexit. While many of the UK sanctions are very similar to the EU equivalents, there are some important differences (for example over the meaning of ‘ownership and control’). Companies will need to review their sanctions compliance and screening procedures.

Internal investigations – key developments

The SFO published its own internal guidance on DPAs, which provides information about the circumstances in which the SFO will consider offering a DPA to a company. There is nothing hugely revealing in the guidance over and above what we have already heard in speeches, inferred from previous DPAs or seen in the CPS DPA Code of Practice. It confirms that cooperation will be considered ‘in the round’. For example, we have seen from previous DPAs that self-reporting misconduct is not a pre-condition to a company being offered a DPA. The guidance confirms that self-reporting within a reasonable time is an important aspect of cooperation but a failure to do so is not a bar to a DPA. Previous cases have shown that a failure to self report can be atoned for by later exceptional cooperation. Even a failure to offer exceptional cooperation throughout does not preclude a DPA, although it may affect the fine discount – a DPA entered into in 2020 contained a fine discount of 40% (rather than the more common 50%) as the company was said to have only fully cooperated quite “late in the day”. There will of course be other factors to take into account on the delicate decision of whether to self-report, such as whether corporate liability (absent a failure to prevent offence) is likely to be proved and whether there are already obligations to report to another authority (eg a regulator or because of AML concerns).

On privilege and waiver, the guidance confirms that waiving privilege will be seen as cooperative, but a company cannot be penalised for not waiving privilege.

For evidence collection and review during an internal investigation which involves data being transferred to the UK from an EU Member State, the EU/UK Trade and Cooperation Agreement contains a four to-six-month transition period on data protection, during which time the UK is not treated as a “third country” under the EU GDPR. This means that, for now, businesses do not need to change their compliance processes regarding transfers of personal data between the UK and the EU. It is hoped that during this transition period we will see the European Commission make a decision on the adequacy of the UK’s data protection laws allowing for free transfer on a more permanent basis. The UK had already indicated separately and independently that it regards the EU as offering adequate protection.
Sectors targeted by law reforms or enforcement action

There will inevitably be pressure on law enforcement bodies to prioritise investigations into pandemic-related crime during 2021. This may result in the SFO taking forward more fraud cases than new bribery cases in the short term. The FCA will be keen to investigate allegations of market abuse during the pandemic. Outside pandemic-related enforcement:

– We expect to see greater focus on tax evasion enforcement. For the ‘failure to prevent’ facilitation of tax evasion offence HMRC (which is responsible for domestic tax evasion offences, while overseas tax evasion falls within the SFO’s remit) reports that it has 13 corporate investigations ongoing across a range of sectors, and 18 live opportunities under review.

– We expect to see FCA enforcement in the UK related to Cum-ex. The FCA has been carrying out a number of investigations relating to Cum-ex9, whereby shares have been traded quickly to earn duplicate tax refunds on dividend payments. There are related investigations throughout Europe. Any financial institution with the potential for cum-ex exposure (eg if it has a dividend arbitrage desk) should assess its exposure.

– While we are yet to see FCA criminal enforcement of AML breaches, in 2020 there were some very large corporate fines for AML systems and controls failings. AML enforcement may receive a boost if the government delivers on its plans to overhaul the suspicious activity reporting regime. This may help to deal with the OECD recommendations in the Phase 4 Report (March 2019) for the UK to improve corruption detection through AML reporting mechanisms. If implemented, this may lead to an increase in financial crime being detected from SARs.

Financial crime issue predictions for 2021

Post-Covid-19: crime rises when individuals are under financial pressure. The combination of remote working, reduced compliance budgets, volatile markets and financial pressure may lead to increased risk of financial crimes such as market abuse, fraud and misleading the market. GCs will need to be agile to respond to this risk, and ensure that compliance policies and speak-up programmes are refreshed and firmly embedded culturally in their organisations.

Delay: the UK’s coronavirus lockdown has had an impact on the ability of some authorities to effectively pursue their investigations. We expect to see a knock-on effect on charging decisions going forward. More prolonged SFO investigations are likely to result despite the SFO wanting to speed up its work. This is not good news for companies and individuals who are currently the subject of already lengthy investigations.

Brexit: we may see businesses seek to penetrate new markets, clients and industry sectors in 2021. This may bring a higher corruption risk.

Culture: The only defence for corporates faced with bribery or facilitating tax evasion allegations is ‘adequate’ or ‘reasonable’ procedures. We expect to see a focus on the non-executive and senior board members’ tone from the top and corporate culture as authorities probe just how embedded compliance policies and procedures are. Senior managers may also be asked about the ‘tone from the middle’ or, as the FCA has termed, the ‘tone from within’.

Disputes on privilege issues, and access to documents and data held abroad will continue.

Careful trade-off is required when considering whether to self-report wrongdoing, taking into account the cost/benefit analysis of a DPA and enforcement risk.

Data protection questions will inevitably remain in cross-border investigations, read more.

---

9 Bloomberg reports 14 active investigations into firms, and six into individuals, by the FCA.
“Highly reputed across compliance and regulatory investigations, including anti-bribery matters. Experienced advisers on corruption and money laundering allegations, alongside sanctions.”

Chambers UK 2021, Financial Crime: Corporates

“Allen & Overy LLP ‘s corporate crime team is ‘practical and pragmatic’, and is as adept at representing large multinational companies as well as international financial institutions in business-critical investigations.”

Legal 500 UK 2020, Regulatory Investigations and Corporate Crime

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

**Jonathan Hitchin**  
Partner – London  
Tel +44 20 3088 4818  
jonathan.hitchin@allenovery.com
U.S. enforcement activity was down overall in 2020, with some notable exceptions. The overall scale of white collar criminal prosecutions in 2020 reached a record low. However, FCPA enforcement remained active, there was a burst of enforcement activity in the crypto space, and the size of financial penalties remained substantial. We also saw an increase in activity in antitrust enforcement and sanctions activity.

In terms of policy, the DOJ and the SEC have become more transparent about the requirements of cooperation credit and have increased transparency and guidance for FCPA investigations. Enforcement focus was particularly evident with respect to healthcare and biotech industries, social media companies, the financial services industry, and cryptocurrency.

The U.S. continues to increase its cooperation and coordination with other authorities as part of the investigation process. While President Trump’s administration winds down, we expect that President elect Joe Biden’s Justice Department will ramp up white collar crime enforcement, returning to a practice of increased scrutiny of corporate wrongdoing.

Investigations trends/developments

Enforcement agencies have signalled an intention to focus on pandemic-related misconduct. This shift in focus, coupled with practical limitations arising out of the pandemic, temporarily slowed traditional white collar crime enforcement. Trends later in 2020 showed that enforcement agencies are resuming their focus on other areas of white collar crime.

Enforcement agencies continued to focus on spoofing cases, principally in markets for precious metals futures, like gold and silver.

In 2020, white collar criminal prosecutions reached their lowest numbers in around 35 years. The vast majority of the DOJ’s white collar cases involved individual prosecutions, rather than institutional or corporate prosecutions, a focus that the DOJ has emphasised throughout the last few years. The latest available data shows that criminal white collar crime prosecutions dropped by nearly 50% in 2020, however, that decline may be short-lived.

The U.S. Securities and Exchange Commission (SEC), the U.S. Commodities Future Trading Commission (CFTC), the Financial Crimes Enforcement Network (FinCEN), and the Consumer Finance Protection Bureau (CFPB) remain active in enforcement and investigations, as do state regulators:

– The SEC brought suits arising from alleged insider trading, violations of the Foreign Corrupt Practices Act (FCPA), market manipulation, and various violations of securities offerings. The SEC initiated 715 enforcement actions in Fiscal Year 2020, down from 862 such actions in Fiscal Year 2019.
Most CFTC enforcement cases involved retail fraud. Sixteen of the actions involved manipulative conduct cases alleging efforts to manipulate the price of a swap or commodity. Nine actions involved failure to register cases and/or illegal “off exchange” contracts cases.

FCPA enforcement has remained a clear and consistent priority of the SEC and DOJ. Although the number of FCPA enforcement actions are down, the breadth of enforcement in terms of countries and industries and the severity of penalties indicate that the enforcement agencies are still active. Settled corporate actions by enforcement agencies resulted in more than USD7.6bn in fines, penalties, and disgorgement. The DOJ and the SEC published an updated version of the FCPA resource guide, which emphasises cooperation and coordination among additional law enforcement partners in the U.S. and abroad.

Sanctions activity by OFAC continues to be a hotspot in U.S. enforcement activity, with a key focus on activity in Cuba, Venezuela, Iran, and North Korea. OFAC announced over ten settlements this year, primarily for compliance failures and failures to have adequate controls and screening procedures – at least, in part, some of these violations were due to automated screening system failures or deficiencies. Non-U.S. persons who process financial transactions to, through or involving U.S. financial institutions that relate to commercial activity with an OFAC-sanctioned country, region or person, may be – and have been – penalised by OFAC for violating U.S. sanctions. Companies operating in higher-risk jurisdictions should be sensitive to sanctions compliance by tracking developments with sanctions regulations, ensuring they understand the full scope of sanctions prohibitions, and dedicating sufficient resources to U.S. sanctions compliance.

AML: U.S. authorities continued to focus on holding financial institutions to account for AML deficiencies and have also begun to flex the jurisdictional boundaries of their affirmative money laundering rules. Those that require financial institutions to implement and maintain effective anti-money laundering programmes have limited extraterritorial jurisdictional reach and in most cases apply solely to domestic financial institutions. In contrast, those that prohibit the affirmative use of the U.S. financial system as a conduit for criminal proceeds have broad extraterritorial reach.

The DOJ’s FIFA-related money laundering action against a major non-U.S. financial institution is an example of a money laundering investigation against a foreign financial institution (within its jurisdictional reach); the DOJ then imposed, through its settlement with the foreign institution, obligations to adhere to U.S. anti-money laundering requirements, which the institution would not otherwise be automatically subject. We expect heightened AML enforcement to continue in 2021.

Compliance programmes: U.S. authorities have continued to emphasise the maintenance of effective compliance programmes, with evolving expectations and greater transparency offered by the enforcement agencies. These updates reflect an emphasis on a continuous, rather than snapshot, assessment of compliance efforts, the increased importance of a process to track and incorporate lessons learned into the risk assessment and management, and an expectation that companies will take advantage of data analytics in developing robust compliance programmes.

The DOJ updated its guidance on the Evaluation of Corporate Compliance Programmes. While the updates are not extensive, they reflect the DOJ’s continued emphasis on the practical approach to evaluating the effectiveness of a company’s compliance programme. It is not enough to make sure that a programme is in place, but companies should continually seek to ensure that the programme is working. For example, the compliance update no longer asks whether a compliance programme is implemented effectively, but instead questions whether a company’s programme is “adequately resourced and empowered to function effectively”. Corporates should consider whether there are adequate resources and empowerment within the company to ensure effective implementation of a compliance programme by looking at data points, including the number and experience level of compliance functions within an organisation, their reporting lines, and the resources available to the compliance function. Companies are expected to implement and test a corporate compliance programme that evaluates and revises the risks that companies face on an ongoing basis, rather than focus on risks from a single point in time.
Significant law reforms impacting corporate criminal liability

The U.S. Congress is considering significant changes to the U.S. anti-money laundering programmatic requirements. Late in 2020, the U.S. Congress passed the “National Defense Authorization Act for Fiscal Year 2021” (H.R.6395). The bill contains a beneficial ownership provision (Section 6403) that, if signed into law by the President, would require corporations to identify and disclose who owns and controls them to FinCEN. The bill also includes a provision (Section 6314) that would create a new Bank Secrecy Act (BSA) whistleblower programme at the Treasury. As of this writing, it is unclear whether or not the President will veto the bill, and, if so, how Congress will respond.

Internal investigations – key developments

As highlighted in the 2020 FCPA Resource Guide, the DOJ continues to provide strong incentives for companies to timely and appropriately disclose and remEDIATE misconduct and limits for credit offered if a company fails to meet its requirements. Companies should closely consider such incentives for voluntary disclosure. The DOJ has stated that these principles are meant to guide companies of “all shapes and sizes – from small businesses transacting abroad for the first time to multinational corporations with subsidiaries around the world”.

The DOJ and the SEC expect company investigations to be more robust than in the past, and to address previous wrongdoing in the growth of compliance programmes. The Guide further emphasises acquirer compliance measures in M&A transactions and includes a formal incentive structure to encourage acquirers to voluntarily disclose wrongdoing uncovered at subsidiaries in return for presumed declinations. Timely and comprehensive risk-based due diligence remains crucial to prevent the continuation of any misconduct, to mitigate liability for past conduct, and to ensure proper training and integration.

Data privacy laws impact how data can be treated during an internal investigation. 2020 saw increased regulation. California and New York are the first states to enact broad legislation, but many other U.S. states are also considering data privacy laws. Members of the U.S. Senate have proposed sweeping federal privacy legislation, the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act. SAFE DATA seeks to provide individuals with additional protection and control, directs businesses to increase transparency and accountability, and to strengthen the Federal Trade Commission’s enforcement power.

Sectors targeted by law reforms or enforcement action

Prior to the start of the Covid-19 pandemic, there was a heightened focus by enforcement agencies and lawmakers on social media companies, technology companies, financial institutions and financial services, and financial-tech hybrid companies – with an emphasis on cryptocurrency. The Covid-19 pandemic appears to have diverted some attention of both lawmakers and enforcement agencies. We expect to see a particular focus, at least temporarily, on Covid-19-related areas, including healthcare, pharmaceuticals, false claims, advertising by companies operating in the healthcare field, and companies operating in the healthcare and biotech space.

However, the focus on financial institutions and financial services has not abated, and this may well be a focus of the new administration. In a landmark settlement, JPMorgan Chase entered into a resolution with the DOJ and the CFTC in return for a record fine of USD920m for spoofing and manipulation violations. This action is an example of enforcement authorities’ continued focus on trading activity such as spoofing and insider trading.
Enforcement agencies are also focusing on cybercrime and cryptocurrency, particularly by the SEC and the DOJ. Telegram, a messaging service, entered into a settlement with the SEC and agreed to pay a USD18.5m penalty to the SEC, and to return USD1.2bn to its investors over the unregistered offering of digital tokens. Kik Interactive, a Canada-based messaging platform, paid a USD5m penalty for launching an illegal Initial Coin Offering and breaking securities laws. There have also been a number of criminal actions – the DOJ announced a criminal indictment against executives of a cryptocurrency platform, alleging money laundering charges and Bank Secrecy Act violations. The CFTC has filed a civil enforcement action against the same cryptocurrency trading platform for the alleged operation of an unregistered trading platform and for alleged violations of CFTC regulations, including failure to implement required anti-money laundering procedures. Corporates operating in this space should be cautious of their perceived status as exchanges or as money services businesses, and the regulatory requirements that follow.

Considerable resources have been directed toward Covid-19-related fraud, microcap fraud, insider trading, market manipulation, and false or misleading issuer disclosures, which intersect with many of the existing enforcement priorities.

Cross-border coordinated enforcement activity

United States authorities have worked increasingly with international authorities in parallel investigations. In 2020 coordination was formalised in the announcement of several new cross-border coordination initiatives.

First, in mid-2020, the bilateral agreement between the United States and the United Kingdom on Access to Electronic Data for the Purpose of Countering Serious Crime entered into force. The agreement permits criminal authorities in the United States and the United Kingdom to obtain electronic data directly from a range of telecommunications companies (called Covered Providers) from each country without any need to go through the domestic authorities in each respective country, a mutual legal assistance treaty (MLAT) or any other cumbersome and time-consuming routes currently used. This development could have a significant impact on any United States company whose business satisfies the definition of Covered Provider including, for example, social media platforms, data hosting, storage and processing, cloud storage, or potentially any other company to the extent it provides clients with an ability to communicate, process, or store data. Read more here.

Second, the DOJ signed a Memorandum of Understanding (MOU) with the Korean Prosecution Service, formalising cooperation and coordination on international cartel investigations. This agreement comes amidst an increased focus on cooperation with foreign law enforcement agencies in criminal cartel matters by the DOJ’s Antitrust Division.

A recent example of coordinated cross-border enforcement activity is the coordinated settlements between a large aerospace company, the DOJ, the UK Serious Fraud Office, and France’s Parquet National Financier on 31 January 2020. All three enforcement agencies agreed to suspend formal criminal proceedings against the company in return for a commitment to implement commonly agreed sanctions, which included the payment of fines of up to USD4bn, the appointment of external compliance monitors, and serious corporate governance reforms.

Companies should remain aware of the potential for multiple settlements and penalties, and prepare a comprehensive strategy to navigate these challenges as the start of any investigation.
Our predictions for 2021 are:

- An increase in criminal and civil investigations during the Biden Administration, starting in 2021.
- Antitrust will continue to be a key enforcement area. In 2020, we saw major antitrust filings by the DOJ against Google, and by the DOJ and 48 states against Facebook, seeking divestiture of the social media platform, Instagram, and the messaging platform, WhatsApp.
- An increased focus by enforcement agencies in the healthcare field.
- An increase in regulatory and enforcement action and investigations not just related to the stimulus programmes and other coronavirus relief efforts, but also as a result of conduct related to turbulent market conditions. There will likely be an increase in investigations of alleged fraud schemes, such as mismarking fraud, and into accounting and financial disclosure issues.
- We expect that enforcement agencies will continue to target traditional market abuses like insider trading, spoofing and other trading conduct.
- Particular scrutiny by the SEC of company disclosures (or purported omissions) made during the pandemic. The SEC has warned that insiders are “regularly learning” new material non-public information that may “hold an even greater value than under normal circumstances”. Public companies should verify that there are robust policies and procedures in place designed to prevent the misuse of material non-public information and ensure that disclosures adequately address risks created by Covid 19.

“They’re great and they do an enormous amount of work. They do a lot of interesting work across the spectrum. They’re terrific and at the top of the heap.”


“He [David Esseks] is really amazing. He is the picture of credibility. He is persuasive and great on his feet: it’s extremely impressive.”


“I like him [Gene Ingoglia] a lot. He is a smart and creative lawyer who has a lot of credibility and is versatile. He’s a good lawyer and investigator and should be in the rankings.”

### Key team members

<table>
<thead>
<tr>
<th>Name</th>
<th>Position – City</th>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Esseks</td>
<td>Partner – New York</td>
<td>Tel +1 212 610 6326 <a href="mailto:david.esseks@allenovery.com">david.esseks@allenovery.com</a></td>
</tr>
<tr>
<td>Ken Rivlin</td>
<td>Partner – New York</td>
<td>Tel +1 212 610 6460 <a href="mailto:ken.rivlin@allenovery.com">ken.rivlin@allenovery.com</a></td>
</tr>
<tr>
<td>Eugene Ingoglia</td>
<td>Partner – New York</td>
<td>Tel +1 212 610 6369 <a href="mailto:eugene.ingoglia@allenovery.com">eugene.ingoglia@allenovery.com</a></td>
</tr>
<tr>
<td>Julian Moore</td>
<td>Partner – New York</td>
<td>Tel +1 212 610 6309 <a href="mailto:julian.moore@allenovery.com">julian.moore@allenovery.com</a></td>
</tr>
<tr>
<td>Kuang Chiang</td>
<td>Associate – Washington, D.C</td>
<td>Tel +1 202 683 3868 <a href="mailto:kuang.chiang@allenovery.com">kuang.chiang@allenovery.com</a></td>
</tr>
<tr>
<td>Maura Rezendes</td>
<td>Partner – Washington, D.C</td>
<td>Tel +1 202 683 3864 <a href="mailto:maura.rezendes@allenovery.com">maura.rezendes@allenovery.com</a></td>
</tr>
<tr>
<td>William Jacobson</td>
<td>Partner – Washington, D.C</td>
<td>Tel +1 202 683 3883 <a href="mailto:william.jacobson@allenovery.com">william.jacobson@allenovery.com</a></td>
</tr>
<tr>
<td>Jonathan Lopez</td>
<td>Partner – Washington, D.C</td>
<td>Tel +1 202 683 3888 <a href="mailto:jonathan.lopez@allenovery.com">jonathan.lopez@allenovery.com</a></td>
</tr>
<tr>
<td>William E. White</td>
<td>Partner – Washington, D.C</td>
<td>Tel +1 202 683 3876 <a href="mailto:william.white@allenovery.com">william.white@allenovery.com</a></td>
</tr>
<tr>
<td>Claire Rajan</td>
<td>Senior Counsel – Washington, D.C</td>
<td>Tel +1 202 683 3869 <a href="mailto:Claire.rajan@allenovery.com">Claire.rajan@allenovery.com</a></td>
</tr>
<tr>
<td>Rebecca Delfiner</td>
<td>Associate – New York</td>
<td>Tel +1 212 756 1194 <a href="mailto:rebecca.delfiner@allenovery.com">rebecca.delfiner@allenovery.com</a></td>
</tr>
<tr>
<td>Laila Delimustafic</td>
<td>Associate – New York</td>
<td>Tel +1 212 756 1178 <a href="mailto:laila.delimustafic@allenovery.com">laila.delimustafic@allenovery.com</a></td>
</tr>
<tr>
<td>Jiayi Lin</td>
<td>Law Clerk – New York</td>
<td>Tel +1 212 756 1122 <a href="mailto:jiayi.lin@allenovery.com">jiayi.lin@allenovery.com</a></td>
</tr>
<tr>
<td>Jonathan Wong</td>
<td>Law Clerk – New York</td>
<td>Tel +1 212 756 1168 <a href="mailto:jonathan.wong@allenovery.com">jonathan.wong@allenovery.com</a></td>
</tr>
</tbody>
</table>
GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,500 people, including some 550 partners, working in over 40 offices worldwide. **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.

© Allen & Overy LLP 2021. This document is for general guidance only and does not constitute advice.