

Self-reporting: What multinational corporations need to know

Simon Airey, Edward Diskant and Nicolette Kost De Sèvres

McDermott Will & Emery

17 May 2024

This is an Insight article, written by a selected partner as part of GIR's co-published content. [Read more on Insight >](#)

In summary

This article summarises some of the key benefits and risks of self-reporting in the United States, the United Kingdom and France, drawing out the principal similarities and differences between these three key jurisdictions. Recent pronouncements by each country suggest increasing harmonisation in their approaches, perhaps to make the investigation of multinational corporations more consistent and cross-border enforcement more effective; however, there are a number of key differences of which companies should be aware.

Discussion points

- Self-reporting regimes in the United States, the United Kingdom and France

Referenced in this article

- US Department of Justice (DOJ)
- DOJ Justice Manual
- Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy
- Serious Fraud Office
- FCA Handbook
- DPA Code of Practice
- National Financial Prosecutor's Office
- French Anti-Corruption Agency
- Sapin II Law

Companies that have uncovered potential wrongdoing will often find themselves having to make a difficult choice: do they aim to resolve the issue in private (with the risk that the matter will subsequently come to the attention of the authorities) or should they self-report voluntarily (setting in motion an external investigation, the result of which is unknown and potentially very damaging)? The consequences of such a decision can have an impact many years into the future, posing potentially long-term reputational, financial and legal risks.

The assessment of the risks and rewards of either option increasingly requires companies to take a multi-jurisdictional approach. Even where the relevant conduct may have been confined to a single jurisdiction, companies with cross-border operations must consider their legal exposure across a range of jurisdictions, as well as the appetite of the authorities in each relevant country to investigate, should they become aware of the matter.

This is all the more so as key jurisdictions have passed new laws with wide extraterritorial effect, enforcement authorities have shown themselves willing and able to cooperate closely with their international counterparts, and legal regimes have evolved to incentivise prompt self-reporting (and impliedly sanction companies that do not). The result is that companies can no longer take a siloed national approach but rather must consider strategy in the round.

This article summarises some of the key benefits and risks of self-reporting in the United States, the United Kingdom and France, drawing out the principal similarities and differences between these three key jurisdictions. Recent pronouncements and enforcement trends in each country suggest increasing harmonisation in their approaches, perhaps to make the investigation of multinational corporations more consistent and cross-border enforcement more effective; however, there are a number of key differences of which companies should be aware.

United States

While there continues to be no formal requirement under US law to self-report potential wrongdoing, the Department of Justice (DOJ) continues to issue guidance making clear that voluntary self-disclosure is paramount for the DOJ to impose lesser sanctions where there has been misconduct and offering real benefits for those that choose to self-disclose. This new

guidance includes more detail to policies set forth in the DOJ's manual for federal prosecutors (the JM), which has long provided that 'prosecutors may consider a corporation's timely and voluntary disclosure, both as an independent factor and in evaluating the company's overall cooperation'.^[1]

As the guidance makes clear, and notwithstanding the 'voluntary' label, DOJ leadership is placing increased emphasis in recent years on self-reporting, highlighting various incentives and benefits to doing so and warning of increased sanctions for those who do not. The DOJ Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy (the Policy or the Corporate Self-Disclosure Policy), released in early 2023 and applicable to all corporate criminal matters handled by the Criminal Division, spells out those benefits, which can include more favourable settlement terms, including non-prosecution or deferred prosecution agreements (DPAs), and reduced financial penalties.^[2] Perhaps most importantly, the Policy provides that 'when a company has voluntarily self-disclosed misconduct to [the DOJ], fully cooperated, and timely and appropriately remediated . . . there will be a presumption that the company will receive a declination absent aggravating circumstances involving the seriousness of the offense or the nature of the offender'.^[3] By contrast, companies that choose not to self-report face the prospect of criminal indictment, which can itself be ruinous even before fines and penalties are imposed.

However, companies must still balance the potential benefits of self-reporting with the risks posed by disclosing potentially criminal conduct to an enforcement authority, often before even the company itself can understand all of the facts.

Further, when determining whether to self-report, companies should consider the potential effects of new whistle-blower incentives recently announced by the DOJ.^[4] The new whistle-blower programme, which the DOJ promises to formally launch as a pilot programme in late 2024, will offer financial incentives, likely in the form of a portion of the DOJ's ultimate recovery, to individuals who report misconduct relating to financial crimes and foreign and domestic corruption.^[5] The programme is intended to 'fill gaps' that were not previously addressed by existing whistle-blower programmes, and provides another reason for companies to enhance their compliance programmes to detect issues when they arise and to voluntarily self-disclose misconduct when they learn of it.

For companies facing the prospect of a self-report, the benefits noted above must be weighed carefully against the daunting work that US authorities require of companies seeking self-disclosure and cooperation credit.

First, with respect to timing, the DOJ requires companies considering self-reporting to make that decision quickly, mandating that a company make a disclosure 'within a reasonably prompt time after becoming aware of the misconduct' and 'prior to an imminent threat of disclosure or government investigation'.^[6] If what the DOJ considers to be 'aggravating' circumstances are present, including, for example, involvement by executive management or a significant profit resulting from the misconduct, the company's disclosure must be made even sooner or 'immediately upon the company becoming aware of the allegation of misconduct' to maintain eligibility for a declination.^[7] While companies frequently face pressure to self-report conduct before knowing all of the facts, the DOJ's increasing focus on speed may exacerbate that tension in circumstances where a company needs to investigate matters thoroughly before reporting something of potential significance and consequence.

The DOJ's new Self Harbor Policy provides even more specific guidance regarding the appropriate timing of a self-disclosure made in the context of a merger or acquisition.^[8] Under the Safe Harbor Policy, companies that uncover misconduct during pre-acquisition due diligence of the target entity will receive a presumption of declination from the DOJ if they disclose such misconduct within six months of closing the transaction, remediate the misconduct within one year of closing and cooperate with the DOJ during any investigation.^[9]

Second, the DOJ requires that companies seeking to self-report under the Corporate Self-Disclosure Policy and related guidance must provide 'all relevant, non-privileged facts known to it, including all relevant facts about individuals involved in or responsible for the misconduct'.^[10] This self-report must be made with regard to all 'all individuals . . . inside and outside of the company regardless of their position, status or seniority'.^[11]

Third, the Policy requires 'full cooperation' following disclosure.^[12] This aspect of the Policy typically requires a prompt, robust internal investigation by the company's counsel and includes an ongoing obligation to disclose 'all non-privileged facts relevant to the wrongdoing at issue',^[13] which includes facts gathered during such an internal investigation, attribution of those facts to specific sources as opposed to a general narrative and timely updates regarding the internal investigation (including, again, identification of individuals involved in the wrongdoing and details regarding their conduct). The DOJ has made clear that cooperation is expected to be 'proactive rather than reactive' and that the company should go so far as to be aware of and identify 'opportunities for [the DOJ] to obtain relevant evidence not in the company's possession and not otherwise known to [the DOJ]'.^[14]

'Full cooperation', according to the Policy, also requires timely and voluntary preservation, collection and disclosure of relevant documents and information including disclosure of overseas documents and information as well as 'facilitation of third-party production of documents' and translations of relevant documents.^[15] Where the provision of overseas documents or information may be restricted because of data privacy rules or blocking statutes, the company bears the burden of establishing the existence of such restrictions and is required to identify 'reasonable and legal alternatives' to assist the DOJ in obtaining the information.^[16] Companies seeking full cooperation credit are expected, consistent with their individual rights under US law, to make employees available for interviews with the DOJ.

In addition, companies should be aware of new policies from both the DOJ and the Federal Trade Commission (FTC) with respect to ephemeral messaging. In March 2023, the DOJ revised its guidance on corporate compliance programmes to note that it would consider whether company policies governing messaging applications such as Slack, Teams or Zoom, and Bring Your Own Device policies are 'tailored to the corporation's risk profile and specific business needs'.^[17] Additionally, the DOJ emphasised the need for companies to bolster policies regarding ephemeral data preservation, noting that companies should work to ensure 'to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation'.^[18]

Then, in January 2024, the DOJ and the FTC imposed affirmative obligations on companies to preserve communications on ephemeral messaging platforms during any investigation or litigation by the DOJ's Antitrust Division or the FTC.^[19] These new requirements may ultimately require policy changes by companies that have automatic deletion in place for these types of communications and are not only a key consideration for companies working to ensure that they are meeting the DOJ's standards for 'full cooperation' but crucial for companies to avoid obstruction of justice charges.

Fourth, any company that self-discloses must be prepared to subject its compliance programme to heavy scrutiny. Indeed, in conjunction with announcing recent changes to the Corporate Self-Disclosure Policy, DOJ leaders have emphasised that 'voluntary self-disclosure is an indicator of a working compliance program and a healthy corporate culture', adding that 'companies who own up will be appropriately rewarded in [the DOJ's] approach to corporate crime'.^[20] Conversely, senior DOJ leaders have warned even more recently that, for companies whose compliance programmes are not current or adequate, their failure to proactively improve and enhance their compliance function will 'cost them down the line'.^[21]

Consistent with that guidance, and as part of engagement with the DOJ following a self-disclosure, companies will be expected to provide details regarding their compliance programme, both at the time of the misconduct and at the time of resolution. Moreover, the Policy expressly requires that companies seeking cooperation credit establish that they have engaged in 'timely and appropriate remediation',^[22] including improvements to the compliance function as needed.

Fifth, DOJ leadership implemented its three-year Pilot Program on Compensation Incentives and Clawbacks (the Pilot Program) in March 2023, requiring companies to 'develop compliance-promoting criteria within its compensation and bonus systems', making clear that the compensation system will also be scrutinised as part of any DOJ resolution.^[23] Under the Pilot Program, the DOJ requires all corporate resolutions to include compliance enhancements directly relating to the remuneration and bonus system, including prohibitions on bonuses for employees who do not satisfy 'compliance performance requirements' and disciplinary measures to be imposed on those employees who violated the law, as well as those who had supervisory authority over the employees or business area that engaged in the misconduct or were 'wilfully blind' to it.^[24] Even if a criminal resolution is warranted, if a company demonstrates that it has implemented a programme to recoup compensation from employees engaged in wrongdoing, any fines imposed will be reduced.^[25]

Taken collectively, these requirements impose substantial burdens on companies seeking to self-report and therefore require careful consideration when evaluating whether a 'voluntary' self-disclosure is appropriate and in the company's best interests. Indeed, while the DOJ's heavy emphasis on voluntary self-disclosure makes clear its own position on self-disclosure, it is not always clear for a company whether voluntary self-disclosure is in its own interest, particularly in the early stages of efforts to investigate potential misconduct. Companies must be particularly attuned to the early stages of an internal review, where the decision to self-report is frequently made, and weigh the possibility that making the decision to disclose too early – especially before enough facts are known to make an informed decision – may result in unnecessary scrutiny from enforcement agencies and potential reputational harm to the company that may be avoidable and unwarranted.

United Kingdom

In certain respects, the position in the United Kingdom is similar to that in the United States; however, key areas of difference include (1) the wider set of specific circumstances in which there can be a formal obligation to self-report to relevant authorities and (2) the narrower set of potential benefits of choosing to do so. In particular, in contrast to the position in the United States, formal declinations are not available in the United Kingdom, with the key benefits of a voluntary self-report instead being the increased prospect (but no guarantee) of resolution through a DPA, no criminal conviction and a reduced financial penalty (in addition to 'softer' benefits, such as increased predictability and the ability to better manage any reputational fallout). An additional factor requiring special consideration in the context of the United Kingdom is that reforms in recent months (and reforms that are soon to be implemented) have the potential to increase drastically the scope for potential criminal liability in corporates with touchpoints with the United Kingdom.

While, as in the United States, there is no general obligation to report crime to the authorities, firms regulated by the Financial Conduct Authority (FCA) are under a duty to deal with their regulators in an open and cooperative way and are under an obligation to disclose appropriately 'anything relating to the firm of which the FCA would reasonably expect notice'.^[26] While the FCA accepts that the timing of the notice depends on the circumstances, it expects a firm to 'act reasonably' and discuss relevant matters with it 'at an early stage, before making any internal or external commitments'. In certain cases, the obligation to notify is immediate.^[27]

Obligations to notify may also arise under applicable anti-money laundering and counterterrorist financing rules. Persons working in the 'regulated sector' (a statutory definition that includes those working in the financial sector, lawyers in relation to certain transactions, auditors, tax advisers, casinos and crypto-asset exchanges) must, subject to certain limited exceptions,

submit a suspicious activity report to the National Crime Agency. This duty arises in relation to information that comes to them in the course of their business if they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing, or even just attempting the latter.^[28]

Even if a person does not work in the regulated sector, if they know or suspect that property they are dealing with constitutes or represents a person's benefit from criminal conduct, they are at risk of committing a money laundering offence unless they make an 'authorised disclosure' and seek a formal defence from the authorities (effectively a form of 'consent' to continue with the activity), commonly referred to as a 'defence against money laundering'.^[29]

Other notification requirements may arise under the rules of professional bodies^[30] and licensing authorities^[31] or under data privacy^[32] and sanctions legislation.^[33] Companies with securities listed on regulated markets must also consider whether they are obliged to make any market disclosures (eg, if the fact of the underlying conduct or the findings of the internal investigation may constitute inside information).^[34]

Outside these specific cases, the position in the United Kingdom mirrors that in the United States, in that, while there is no general duty to disclose potential wrongdoing, there is a heavy emphasis on the benefits of doing so voluntarily.

First, while there is no obligation to notify the Serious Fraud Office (SFO) or His Majesty's Revenue and Customs of suspected criminal conduct, self-reporting to these bodies is listed as an example of cooperation (which is a public interest factor against prosecution and in favour of resolution by way of a DPA or an asset recovery power).^[35] That is not to say that a self-report is a prerequisite to obtaining a DPA; indeed, Entain plc did not make a self-report in advance of its landmark DPA with the Crown Prosecution Service, approved by the Crown Court in December 2023, nor did Rolls Royce in advance of its 2017 DPA with the SFO. Importantly, a self-report would be part of what is ultimately a balancing exercise to be undertaken between factors in favour of and against prosecution, meaning that a self-report is not a guarantee that a prosecution will not follow.^[36]

In the applicable guidance, the UK prosecutors emphasise that, to be effective, the self-report should be part of a 'genuinely proactive approach adopted by the corporate management team when the offending is brought to their notice', involving reporting 'within a reasonable time of the offending coming to light' and remedial actions, including (where appropriate) the compensation of victims.^[37]

The reference to 'reasonable time' allows scope for a company to conduct at least a preliminary investigation into a potential issue prior to self-reporting. This was expressly acknowledged in a speech given by the director of the SFO in 2019, who stated that companies 'have a duty to their shareholders to ensure allegations or suspicions are investigated, assessed and verified, so they understand what they may be reporting before they report it'.^[38] The DPA Code of Practice specifically identifies 'reporting the wrongdoing but failing to verify it, or reporting it knowing or believing it to be inaccurate, misleading or incomplete' as a public interest factor in favour of prosecution (and against the granting of a DPA).^[39]

When considering a self-report, the prosecutor must consider the totality of the information the company has provided, the extent to which the offending was previously known to the prosecutor and the extent to which the company is providing it voluntarily (ie, without the threat of imminent disclosure by a third party or compulsion).^[40] When considering whether a self-reporting company has been genuinely proactive, prosecutors will also need to establish whether sufficient information has been provided, including making witnesses available and disclosing the details of any internal investigation (although, while an organisation can gain credit for disclosing a privileged internal investigation report, it should, in theory, not lose credit for having chosen not to do so).^[41] It is also important not to withhold material in a manner that would jeopardise an effective investigation or, where appropriate, prosecution of relevant individuals.^[42]

Second, self-reporting and subsequent cooperation can lead to a reduced financial penalty. Under the sentencing guidelines for corporate offenders for fraud, bribery and money laundering offences, the fact that a company 'co-operated with [the] investigation, made early admissions and/or voluntarily reported offending' is treated as a mitigating feature, which could result in a lower multiplier on the harm figure for the calculation of a fine.^[43] Cooperation (including self-reporting) can also result in an increased discount on the fine, with a discount of 16.66 per cent (additional to the general 33.33 per cent discount for the equivalent of a guilty plea) being granted in a number of DPAs in recognition of 'extraordinary' cooperation. Likewise, the Office for Financial Sanctions Implementation has set out that a prompt and complete voluntary disclosure can result in up to a 50 per cent reduction on the baseline penalty.^[44]

Third, as in the United States, self-reporting is increasingly seen as a requirement for an effective compliance framework and a signal of an appropriate corporate culture. In the DPA agreed by the SFO and Amec Foster Wheeler Energy Limited, the judge held that the 'proper course' for the relevant company would have been to self-report to the SFO 'not as a matter of legal duty, but as a matter of ethical corporate governance'. While the judge acknowledged that there was no legal requirement to report suspected crime to the authorities, he stated that 'there is a moral duty on all citizens in this respect which extends at least equally to corporations. This failure by the board [to do so] was deplorable'.^[45] As a result, directors may increasingly need to consider whether a voluntary disclosure may, in effect, be required as a matter of proper corporate governance or to comply with their duties to promote the success, and act in the best interests, of the company.^[46]

Balanced against this, a number of cases have demonstrated that a DPA and the full 50 per cent discount to the financial penalty may still be secured in the absence of a self-report, as expressly noted by the judge in the Airbus DPA: 'if subsequent self-reporting or co-operation overall, is of a high quality and brings significant wrongdoing to light that would not otherwise

have come to the attention of the authorities, this will be a significant factor in favour of a DPA'.^[47] Nevertheless, the level of cooperation required in those cases has had to be 'exemplary', which, in practice, may mean that companies need to make strategic concessions they might not otherwise have made. Further, it may be assumed that a tactical decision not to self-report and later to compensate (if required) via exemplary cooperation would be looked on poorly by the authorities and be high risk.

Ultimately, the choice of whether to make a voluntary self-report in the United Kingdom may come down to a company's risk appetite. Choosing not to self-report and to remediate in private can have a number of advantages, not least in terms of litigation risk, resource and reputation management; however, it runs the risk that the conduct may otherwise come to the attention of the authorities, in which case the consequences are likely to be considerably worse for the company.

On the other hand, choosing to self-report can significantly increase the likelihood of obtaining a DPA and a significant discount to the financial penalty; however, unlike in the United States, formal declinations are not available, and a self-report therefore would almost certainly expose a company to a risk of substantial fines (and other expenses) that it otherwise might not have faced. Other potential consequences include the risk of civil litigation and adverse reactions from shareholders, bankers, insurers, investors and other stakeholders. While, for some companies, the potential benefits of voluntary disclosure may fall short of what is required to encourage a self-report, for those in regulated industries (where a prosecution or even a charge could lead to a loss of required licences, consents or access to public sector procurements), the choice can be business critical.

It is worth noting in this context that the circumstances in which a corporate can be convicted of a criminal offence in the United Kingdom have increased substantially since 26 December 2023 (and are due to increase even further within the next year). The Economic Crime and Corporate Transparency Act 2023 (ECCTA) has drastically reformed the 'identification principle' under which criminal acts of those acting as a company's 'directing mind and will' (DMW) can be attributed to a company. Generally speaking, only directors of a company could be its DMW; however, reforms in ECCTA mean that certain criminal acts^[48] of senior managers^[49] – acting within the actual or apparent scope of their authority – will be attributed to the companies. This is a much lower bar to liability and represents a seismic change to corporate criminal liability in the United Kingdom.

In addition, ECCTA will introduce a new 'failure to prevent fraud' offence – expected in late 2024 – under which large companies can be liable to an unlimited fine if persons associated with them commit a specified fraud offence while intending to benefit the company or its clients.

The above reforms will no doubt increase the risk of criminal liability faced by corporates with businesses in the United Kingdom, which will, in turn, lead to a higher number of situations in which a self-report needs to be contemplated.

France

In recent years, continental Europe and France have been continuing to strengthen their fight against financial crime and corruption by effectively requiring companies to play a proactive role in detecting and preventing corruption through stronger enforcement, liability of senior management and recent updates regarding self-reporting and cooperation with authorities.

In France, cooperation with authorities, including self-reporting, has not developed at the same speed as in the United States and the United Kingdom. It is mostly with stronger explicit legal requirements regarding compliance systems that France has addressed the need to strengthen the fight against corruption and put ethics and integrity at the forefront to help companies achieve higher ethical standards. Although there is no explicit legal obligation to self-disclose potential misconduct, recent developments clarify the possibility and advantages to do so.

In France, Law No. 2016-1691^[50] (the Sapin II Law) introduced judicial public interest agreements (CJIPs). This innovative approach for France, commonly referred to as the 'French DPA', incentivises cooperation with the French authorities, which may also include the self-reporting of potential misconduct, as further clarified by the French financial prosecutor's office (the National Financial Prosecutor's Office (PNF)).^[51] The CJIP is an agreement that may be proposed by the PNF to a legal person under investigation by the PNF and that allows legal persons to avoid prosecution for certain offences by paying a public interest fine, putting in place a compliance programme under the monitorship of the French Anti-Corruption Agency (AFA) or repairing the harm caused to potential victims.^[52]

The Sapin II Law has also introduced for companies incorporated in France, and foreign companies not headquartered in France, that exceed certain thresholds^[53] strict compliance measures, which are enumerated in article 17 as eight anti-corruption compliance requirements, namely a code of conduct, a whistle-blowing system, corruption risk mapping, third-party due diligence, accounting controls, awareness and training, a disciplinary system and internal controls.

In this context, and regarding the requirement to implement a whistle-blowing system, both the European Union^[54] and France^[55] have demonstrated a strong commitment to reinforcing whistle-blower protections through enhanced requirements and sanctioning, which, in France, may extend to imprisonment. These requirements and sanctions may concern both the company and individuals, including senior management, and could play an important role in considering self-reporting.

Through the Sapin II Law, which also imposed the creation of an anti-corruption regulator, the AFA, France aimed to promote its anti-corruption regime and compliance obligations as one of the strictest in the world. The AFA is the designated regulator overseeing, among other things, the eight anti-corruption compliance obligations.^[56] The AFA has extensive powers of

supervision to investigate companies,^[57] as well as responsibilities to educate and issue guidelines.

The creation of the AFA in 2017 and of the PNF in 2014 demonstrates France's commitment to stronger enforcement, locally and abroad.^[58] Moreover, a general obligation of reporting misconduct exists for public authorities and officials under them, which may influence the decision of companies to self-report.^[59]

On 16 January 2023, the PNF released its updated guidelines on the CJIP (the Guidelines),^[60] providing companies and foreign authorities with more clarity, predictability and transparency in the implementation process of a CJIP, with the aim of reinforcing cooperation with French authorities and highlighting the importance of robust compliance programmes.

To benefit from a CJIP, the company must, among other things, cooperate in good faith, which may be assessed by the following:

- spontaneous disclosure within a reasonable time;
- demonstrating active cooperation by conducting an internal investigation;
- sharing with the PNF the internal investigation's report within a reasonable time;
- spontaneous implementation of a compliance programme; and
- early adoption of corrective measures.^[61]

The PNF specifies that it assesses the element of reasonable time for self-disclosure in light of the time elapsed between the company's knowledge of the facts and its disclosure to the PNF. A company's good faith is additionally demonstrated if the self-disclosure concerns facts of which the PNF was not yet aware.^[62]

Currently, the French CJIP process does not allow natural persons to be included in a CJIP agreement. However, a mechanism named *Comparution sur reconnaissance préalable de culpabilité*, which is a French equivalent of a 'guilty plea' procedure, allows the French public prosecutor to consider a more lenient approach regarding a natural person.

According to the Guidelines, the absence of either a compliance programme, as required under article 17 of the Sapin II Law, or remediation measures, in the case of identified breaches by the AFA, could be considered as unfavourable circumstances for a CJIP. In the assessment of a potential fine, the PNF will assess the level of cooperation of the company in accordance with a set of criteria that may increase or decrease the amount of the fine.^[63] Self-disclosure results in the largest reduction (a maximum reduction of 50 per cent) of the fine.

On 14 March 2023, the AFA and the PNF jointly published a practical guide regarding anti-corruption internal investigations.^[64] Regarding self-disclosure, the guide specifies that a company's early and truthful reporting to the PNF of misconduct and the sharing of the investigation's information will likely reduce the fine in the context of a CJIP, whereas any delay in transmitting the information resulting from the internal investigation or partial communication of the information gathered by the company may be considered as an aggravating factor in the calculation of the fine.

Although self-disclosure is highly incentivised by French authorities, this process still remains relatively rare in comparison with the United States. However, this tendency may change, as we observed more self-disclosure cases in recent CJIPs in 2023.

The AFA has previously referred to self-disclosure considerations for companies in the context of anti-corruption due diligence in mergers and acquisitions.^[65] In its 2021 practical guide,^[66] the AFA indicates the following:

“ If the seller is aware of acts of corruption committed by the target before the transaction, it would also be in its interest to conduct an internal investigation to find out whether it could be implicated as an accomplice or for concealment or laundering of the proceeds of this offence. Where appropriate, the seller could consider reporting itself to the public prosecutor in advance of any report of these acts by the purchaser. ”

Self-disclosure may also be influenced by recent developments in whistle-blower protections, strengthened by a recent EU directive^[67] establishing minimum standards to be transposed nationally, including access to reporting channels both internally (within a company) and externally (directly to authorities).^[68] The Wasserman Law^[69] transposed that directive in France by modifying the Sapin II Law, including requiring companies to provide clear and easily accessible information for whistle-blowers to report externally.^[70]

In July 2023, the AFA published its annual report for 2022,^[71] which confirmed that there has been 'a sharp increase in the number of alerts received by AFA' [unofficial translation]. The annual report mentioned that 'the number of alerts received by AFA increased by 40% (304 reports were received compared with 216 in 2021)'. Among alerts received from non-anonymous whistle-blowers, '83% were from individuals, of whom 68% were from users/residents/citizens, 15% from employees who sometimes identify themselves as whistle-blowers or compliance officers . . . 5% company directors or managers' [unofficial translation].

Overall, in France, the protection of whistle-blowers against retaliation and obstruction and strict confidentiality remain among some of the most important in Europe and abroad and are further safeguarded through strict sanctions, which may include fines and up to two years' imprisonment.^[72] The potential consequences of using an external channel, such as

reporting directly to authorities, are often a catalyst for launching internal investigations that may potentially lead companies to consider voluntary self-disclosure.

Conclusion

As outlined in this article, a key aspect of the regulatory regimes in the United States, the United Kingdom and France has been to reduce the uncertainty of what may follow a self-report and, in doing so, shift the balance in favour of voluntary disclosure. The question remains, however, whether the benefits of voluntary disclosure are sufficiently compelling to offset the hard truth that it may bring issues to the attention of the authorities that they might not otherwise become aware of (and thereby expose a company to legal risks that might otherwise never eventuate).

The United States goes furthest, offering the significant prize (absent aggravating circumstances) of a presumed declination for companies that self-report within a 'reasonably prompt' time and are then able to pass the daunting threshold of establishing cooperation credit. By comparison, the United Kingdom and France provide for an increased likelihood – but no guarantee – of securing a DPA or CJIP, respectively, following a self-report that is made within a 'reasonable' time (although it can be business critical for companies that operate in regulated industries), which may still involve significant financial and other sanctions that a company remediating in private is unlikely to face.

If companies, as is increasingly common, need to assess the benefits of self-reporting across a number of jurisdictions, a 'lowest common denominator' approach may apply, with the decision to self-report being driven by the jurisdiction with the greatest benefits for voluntary disclosure (or sanctions for failure to do so). These decisions made at the outset of finding a compliance issue can be critical strategically and are often fraught with complexity and nuance.

Companies will likely have to navigate competing obligations and manage fact patterns that are rapidly developing and unpredictable. For example, the existence of information gateways between enforcement authorities across different countries may impact the timing or content of a self-report and whether simultaneous or staggered reports should be made in relevant jurisdictions. Leaks by competitors or whistle-blowers may expedite a decision to engage with authorities, and obligations to make market disclosures may create additional complications and risks when triggered.

In any case, the clear lesson is that companies can and should proactively continue to develop a strong culture of compliance, including fulsome policies and a means to comprehensively implement those policies, to be a front line of defence against corporate crime. Further, when a situation arises in which a discussion regarding self-disclosure is necessary, companies should give careful thought to engaging the right people in that discussion – from compliance to legal and to the board, across all potentially relevant jurisdictions – and to do so quickly. As reflected in the DOJ's ongoing dialogue surrounding corporate crime, time is of the essence, and strategies regarding how to deal with potential wrongdoing should be firmly in place before implementation becomes necessary.

**The authors would like to thank counsel James Dobias and associates Jennifer Levensgood, William Merry, Stavroula Nikolaidou and Rebecca Richardson for their assistance in preparing this article.*

Endnotes

^[1] JM § 9-28.900.

^[2] Id. The Policy was incorporated by reference into the United States Attorneys' Offices Voluntary Disclosure Policy, which was rolled out to all 93 US Attorneys' Offices nationwide on 22 February 2023 pursuant to the directive in the Deputy Attorney General's 15 September 2022 memorandum, 'Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group', which instructed that each component of the DOJ that prosecutes corporate crime should review its policies on corporate voluntary self-disclosure and, if there is no formal written policy to incentivise self-disclosure, draft and publicly share such a policy.

^[3] Id. at 1.

^[4] Deputy Attorney General Lisa Monaco Delivers Keynote Remarks at the American Bar Association's 39th National Institute on White Collar Crime (7 March 2024).

^[5] Id.

^[6] Id. at 3.

^[7] Id. at 2. The Policy notes that even in cases where aggravating circumstances are present, a company may still receive a full declination if it can demonstrate that it (1) immediately made a voluntary self-disclosure upon learning of the misconduct, (2) had an effective compliance programme and system of internal accounting controls that enabled the identification of the misconduct and led to the self-disclosure and (3) provided extraordinary cooperation and remediation. In cases where companies self-disclose but where a criminal resolution is still warranted, the DOJ will still recommend at least a 50 per cent but up to a 75 per cent reduction from the low end of the US Sentencing Guidelines fine range. Id.

^[8] Deputy Attorney General Lisa O Monaco, Remarks as Prepared for Delivery at the Society of Corporate Compliance and Ethics' 22nd Annual Compliance & Ethics Institute (4 October 2023).

^[9] Id.

^[10] Id. at 3.

^[11] Id.

^[12] Id. at 3–4.

^[13] Id.

^[14] Id. at 4.

^[15] Id.

^[16] Id.

^[17] US Department of Justice Criminal Division Evaluation of Corporate Compliance Programs, at 15 (Updated March 2023).

^[18] Id.

^[19] Federal Trade Commission, 'FTC and DOJ Update Guidance That Reinforces Parties' Preservation Obligations for Collaboration Tools and Ephemeral Messaging' (26 January 2024).

^[20] Deputy Attorney General Lisa O Monaco, Remarks on Corporate Criminal Enforcement (15 September 2022).

^[21] Deputy Attorney General Lisa O Monaco, Remarks at ABA's 36th National Institute on White Collar Crime (28 October 2021).

^[22] JM § 9-47.120 at 4.

^[23] Deputy Attorney General Lisa O Monaco, Remarks at ABA National Institute on White Collar Crime (2 March 2023); The Criminal Division's Pilot Program Regarding Compensation Incentives and Clawbacks (3 March 2023).

^[24] The Criminal Division's Pilot Program Regarding Compensation Incentives and Clawbacks (3 March 2023).

^[25] Id.

^[26] Financial Conduct Authority (FCA) Handbook, PRIN 2.1.1R, Principle 11. The FCA Handbook sets out a non-exhaustive list of situations where a firm is under an express duty to submit a notification, including where there has been a significant failure in the firm's systems or controls, there has been a significant breach of a rule imposed by the FCA, employees committed a fraud against a customer, or a significant infringement of any applicable competition law has, or may have, occurred (FCA Handbook, SUP 15.3).

^[27] FCA Handbook, SUP 15.3 and SUP 15.7.11G.

^[28] Proceeds of Crime Act 2002, sections 330 and 331; Terrorism Act 2000, section 21A.

^[29] Proceeds of Crime Act 2002, sections 335, 338 and 340. Similar provisions apply in respect of terrorist financing (Terrorism Act 2000, section 21ZA).

^[30] For example, firms of solicitors are under an obligation to report certain matters to the Solicitors Regulation Authority (SRA), including any potentially serious breach of applicable regulatory requirements by themselves or another SRA-regulated person (SRA Code of Conduct for Firms, Rule 3).

^[31] For example, gambling operators licensed by the Gambling Commission are subject to notification obligations under the Licence Conditions and Codes of Practice.

^[32] For example, data controllers are under a duty to notify the Information Commissioner's Office of personal data breaches 'without undue delay, and where feasible, not later than 72 hours after having become aware of it' (UK General Data Protection Regulation, article 33; Data Protection Act 2018, section 67).

^[33] Reporting obligations in relation to UK sanctions vary depending on the relevant sanctions regime, as enacted by the government using its broad powers under the Sanctions and Anti-Money Laundering Act 2018. By way of example, under Regulation 70 of the Russia (Sanctions) (EU Exit) Regulations 2019, certain firms and institutions are required to report to His Majesty's Treasury where they suspect that a person is designated or has committed an offence under those Regulations.

^[34] EU Market Abuse Regulation (as retained under UK law), article 17; European Securities and Markets Authority, 'MAR Guidelines: Delay in the disclosure of inside information and interactions with prudential supervision'; FCA Handbook, DTR 2.5.

[35] DPA Code of Practice, paragraph 2.8.2(i); SFO Corporate Co-Operation Guidance; SFO Corporate Self-Reporting Guidance; and SFO Operational Handbook Guidance on DPAs.

[36] SFO Corporate Self-Reporting Guidance. In April 2024, the SFO reportedly confirmed that it is working to refresh its guidance on self-reporting, with a view to clarifying the hallmarks of good cooperation and encouraging more corporations to come forward.

[37] Joint Prosecution Guidance on Corporate Prosecutions, paragraph 32; DPA Code of Practice, paragraph 2.8.2(i); SFO Operational Handbook Guidance on DPAs.

[38] Lisa Osofsky, 'Fighting fraud and corruption in a shrinking world', at the Royal United Services Institute in London, 3 April 2019, www.sfo.gov.uk/2019/04/03/fighting-fraud-and-corruption-in-a-shrinking-world.

[39] DPA Code of Practice, paragraph 2.8(vi).

[40] SFO Operational Handbook Guidance on DPAs.

[41] Joint Prosecution Guidance on Corporate Prosecutions, paragraph 32; DPA Code of Practice, paragraph 2.8.2.

[42] DPA Code of Practice, paragraph 2.9.1.

[43] Sentencing Council, Sentencing Guidelines: Corporate Offenders: Fraud, Bribery and Money Laundering, Step 4.

[44] Office for Financial Sanctions Implementation guidance, Monetary penalties for breaches of financial sanctions (June 2022), paragraph 4.8.

[45] *SFO v Amec Foster Wheeler Energy Limited*, 1 July 2021, paragraphs 19 to 20.

[46] See, for example, Companies Act 2006, section 172.

[47] *SFO v Airbus SE*, 31 January 2020, paragraph 68.

[48] Schedule 12 ECCTA sets out the offences to which the reformed identification principle applies. As at the time of writing, there is a Criminal Justice Bill going through its legislative journey, which proposes to subject all criminal offences to the new identification principle.

[49] Comprising individuals playing a significant role in (1) the making of decisions about how the whole or a substantial part of the activities of the body corporate or (as the case may be) partnership are to be managed or organised, or (2) the actual managing or organising of the whole or a substantial part of those activities (section 196 ECCTA).

[50] Law No. 2016-1691 of 9 December on transparency, the fight against corruption and the modernisation of economic life (the Sapin II Law).

[51] National Financial Prosecutor's Office (PNF), Lignes directrices sur la mise en œuvre de la convention judiciaire d'intérêt public, 16 January 2023.

[52] Code of Criminal Procedure, article 41-1-2.

[53] Article 17 of the Sapin II Law (eight compliance measures) applies, among others, to companies with over 500 employees and €100 million in turnover. The whistle-blowing obligations also apply to smaller companies with over 50 employees.

[54] Directive (EU) No. 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

[55] Law No. 2022-401 of 21 March 2022 aimed at improving the protection of whistle-blowers (known as the Wasserman Law).

[56] Sapin II Law, articles 1 and 3.

[57] French Anti-Corruption Agency (AFA), Annual Report 2021.

[58] The European Public Prosecutor's Office was created to address offences that may put at stake the financial interests of the European Union (Regulation (EU) No. 2017/1939 of 12 October 2017).

[59] Code of Criminal Procedure, article 40.

[60] See footnote 45.

[61] *Ibid.*, p.9.

[\[62\]](#) Ibid.

[\[63\]](#) Ibid., p.16.

[\[64\]](#) AFA and PNF, Les Enquêtes Internes Anticorruption, March 2023.

[\[65\]](#) Recent case law in France has updated a long-standing principle regarding the transfer of criminal liability to an absorbing entity. See 2 Cass Crim, 25 November 2020, Case No. 18-86.955. The absorbing entity can now be criminally liable for acts committed by the absorbed company prior to the transaction.

[\[66\]](#) AFA, Anti-Corruption Due Diligence for Mergers and Acquisitions, p. 7.

[\[67\]](#) See footnote 48.

[\[68\]](#) Ibid., articles 9 and 10. The other changes in articles 9 to 19 include the possibility of public disclosure if 'no appropriate action was taken' after having reported internally or externally.

[\[69\]](#) See footnote 49.

[\[70\]](#) Decree No. 2022-1284 of 3 October 2022 on the procedures for collecting and processing whistle-blower reports and establishing the list of external authorities instituted by the Wasserman Law, article 8.

[\[71\]](#) AFA, Annual Report 2022, July 2023, p. 44.

[\[72\]](#) Sapin II Law, article 9.



Simon Airey

Partner
McDermott Will & Emery UK LLP
sairey@mwe.com

[View full biography](#)



Edward Diskant

Partner
McDermott Will & Emery
ediskant@mwe.com

[View full biography](#)



Nicolette Kost De Sèvres

Partner
McDermott Will & Emery
nkostdesevres@mwe.com

[View full biography](#)