

## Tackling Corporate Fraud

10 July 2024

---

Tackling corporate fraud is an increasingly high priority for legislators and enforcement agencies globally.

We describe the landscape and look at areas of focus for regulators; namely, fraud in relations payments, cybersecurity, crypto-assets and greenwashing.

### ***Efforts to tackle corporate fraud***

The UK has introduced landmark corporate crime reform in the [Economic Crime and Transparency Act 2023](#) (“ECCTA”). At the centre of the ECCTA is the introduction of a “failure to prevent fraud” offence, which will hold “large organisations” to account where an associated person commits a fraud offence intending to benefit (whether directly or indirectly) the organisation or any subsidiary (see our blogs [here](#) and [here](#)). The ECCTA has also extended the attribution doctrine to allow corporations to be held accountable for the conduct of senior managers in a wider range of circumstances (see our blog [here](#)). The UK enforcement authorities have been active in securing convictions for fraud and in light of the reforms, we anticipate additional investigations in the forthcoming years. The Serious Fraud Office (“SFO”) has warned as part of its [forward-looking strategy](#) that it intends to take a greater role to tackle fraud ensuring cases progress faster and developing the agencies reputation as a partner of choice to work with for prosecutions domestically and internationally. This follows the SFO’s successful [prosecution](#) of an investment manager for £100 million investment fraud as part of an [investigation into a high-profile corporate fraud](#) and the ongoing investigation into a [multi-jurisdictional investment fraud](#). In a similar vein, [the UK Government’s Fraud Strategy](#) commits £100 million to bolster law enforcement and £400 million to tackle economic crime, with a significant proportion of the funds designated to the new UK Fraud Squad. With Labour winning the general election in the UK, we may see commitment to [David Lammy’s statement](#) to pay whistleblowers for uncovering sanctioned entities hiding cash. Labour has also promised to revamp the UK’s fraud strategy and involve tech platforms in an attempt to reduce and tackle online fraud.

In the EU, France’s highest court has followed other EU jurisdictions by reversing its position on corporate successor liability. As a result, criminal liability can now be passed on to a successor entity in certain cases and white-collar crime and anti-bribery are now an increasingly important part of the M&A process in many deals. Similarly, the French equivalent to a Deferred Prosecution Agreement (*Convention Judiciaire d’Intérêt Public*) created in 2016 is now a well-established tool for corporates to settle criminal investigations. The National Financial Prosecutor’s office has recently published new guidelines to formalise the factors for corporates to be eligible to lower penalties (e.g. self-reporting, cooperation/internal investigations, remedial measures...). However, there is still some uncertainty around the treatment of individuals (e.g. directors, managers) in such cases.

## **Payment fraud**

The elections across the world has incentivised legislators to assess ways to protect consumers from fraud. Consequently, the payment services sector is an area of focus. The UK Payment Systems Regulator [continues to take bold action on Authorised Push Payment \(APP\) fraud](#). As part of forthcoming reforms, the PSR will require banks to reimburse customers in most instances of APP using the Faster Payments System. Whilst the UK is introducing mandatory reimbursement, the EU has proposed similar legislation by way of the third [Payment Systems Directive and Regulations](#), which have the objective of combatting and mitigating payment fraud. The US has opted not to use legislation to tackle payment fraud but has indicated banks should compensate customers in a wider range of cases. With the [Senate Banking Committee](#) recently writing to the leading investment banks requesting that they provide further information on their anti-money laundering and fraud prevention procedures and reimbursement practices in relation to consumer disputes. The Committee warned when requesting this information, that they believe banks should reimburse customers when the bank has failed to monitor or prevent fraudulent transfers. The clear intention is to incentivise banks to provide compensation in a wider range of cases of fraudulent transactions.

## **Cybercrime**

Cybercrime is also a priority for enforcement authorities. In France, a new cyber police agency merging existing services ([Office Français Anti-Cybercriminalité](#), “OFAC”) will now be the preferred point of contact for cross-border cooperation between law enforcement agencies on cybercrime. It will collect reports from the public and should be one of the main law enforcement agencies reporting illegal online content or cybercrime to global technology companies. In the UK, the London [Metropolitan Police](#) (MET) recently infiltrated a large-scale online fraud earlier this year. This follows the UK National Crime Agency led Operation Cronos, which disrupted LockBit, one of the world’s most harmful cyber-crime group that has used ransomware to target victims. The Agency obtained thousands of decryption keys to help victims recover encrypted data.

## **Crypto-assets**

The regulatory landscape for cryptocurrencies has varied significantly across different jurisdictions worldwide, sparking a debate on the most appropriate approach to address widespread crime in this area. The aftermath of the failure of the cryptocurrency exchange FTX and the subsequent prosecution of its founder, Sam Bankman-Fried, has seen a growing consensus on the necessity of a regulatory framework. Currently, in the EU, crypto-assets are principally regulated by the fifth AML Directive (AMLD5), which requires custodian wallet providers and providers of exchange services between virtual currencies and fiat currencies to register in the Member State where they provide services. However, this will change with the introduction of the Markets in Crypto-Assets Regulation ([MiCA](#)), which will become applicable later this year. MiCA will introduce a harmonised and all-encompassing regime covering all crypto-assets. As a result, we will see tighter safeguards in place to address fraud in the crypto-currency market (for a guide to MiCA, please see our [navigator](#)). There are also nationwide efforts to tackle crypto-asset fraud across the EU. For example, various forms of crypto-related fraud are monitored by French authorities (from actual scams to unlicensed practice of crypto exchange in France / unauthorized approach of clients in France or deceptive practices).

In the UK, although the details of a more comprehensive future regime have been published, there are currently two regulatory regimes in force that impose requirements on crypto-asset businesses in the UK. First, in-scope firms must be registered under the Money Laundering Regulations 2017, which broadly replicates the EU's AMLD5. Secondly, the UK has regulated the financial promotion of crypto-assets. It is now a criminal offence in the UK to make a financial promotion in respect of a qualifying crypto-asset unless that financial promotion is exempt or approved by an authorised firm (see our blog posts on the [expanded FPO regime](#) and the Financial Conduct Authority's [rules](#) and [guidance](#)). The UK is now in the process of implementing comprehensive crypto-assets regulations. Unlike the EU, however, the UK is not proposing to introduce an all-embracing framework. Instead, adopting a phased approach whereby existing regulatory frameworks will be modified to capture in-scope crypto-assets over several years.

In the US, while there has been an uptick of enforcement actions and some criminal cases in the crypto space, the regulatory framework is not in the same place as the UK and EU. Regulators are trying to appreciate how they can use existing tools to try and bring effective order to a market that has outstripped the pace of regulatory development. There appears to be limited initiative in establishing a set of comprehensive federal rules that could either complement existing legal frameworks or supersede them. In the absence of a federal framework, regulatory oversight is left to the discretion of individual regulators and states, resulting in an ad hoc and somewhat patchwork approach. New York probably has the most comprehensive set of rules, the BitLicense, and in 2023, the New York Attorney General introduced proposed legislation that would implement a comprehensive new regulatory regime for crypto-assets in the state, including registration requirements for market participants and restrictions on financial promotions by influencers.

### ***Greenwashing***

Greenwashing is an emerging area of importance in preventing corporate fraud. The US has committed to hold organisations and individuals to account for ESG misstatements and omissions. [In May 2022 the Securities and Exchange Commission agreed a settlement with a leading bank in relation to ESG misstatements](#). This echoes enforcement action against another leading [bank, which has been](#) required to pay \$25 million for AML violations and misstatements regarding ESG investments. The UK FCA has confirmed its [anti-greenwashing guidance](#). Financial institutions will now need to exercise additional care when promoting the green credentials of financial products. The introduction of the failure to prevent fraud offence may also see investigations for false statements by corporations about the benefits of their products or services offered. The EU has introduced new offences to address greenwashing, such as regulations on advertising of environmental credentials. Claims such as zero emissions / net-zero or stated goals to reach zero emissions (or reduce emissions) are likely in scope. There will be an EU-wide ["greenwashing" directive](#) that member states must implement during 2026. Companies should also be mindful that misleading commercial practices that do not comply with the new EU Directive can and currently are considered unlawful under current unfair competition law in some Member States, e.g., in Germany. There has also been enforcement action in the EU. Earlier this year, [the Commission](#) and national consumer protection authorities commenced action against 20 airlines for misleading greenwashing practices.

### ***Conclusion***

The global trend is towards more regulation and enforcement action to tackle corporate fraud. The shape that reforms and interventions take, and what impact that will have, remains uncertain, especially with the new Government in the UK and elections in the US and elsewhere. Given the fast-paced and emerging landscape, businesses should monitor developments, agilely adapt where necessary, and be aware of risks, as regulators, and prosecutors, will intervene where necessary.