Financial crime reforms

Creating new risks and challenges for firms

JULY 2025

FRESHFIELDS

The Economic Crime and Corporate Transparency Act has introduced a novel failure to prevent fraud offence, as well as extending the criminal attribution doctrine to hold large firms liable for the actions of a wider range of senior managers. In this article the authors consider these reforms as well as areas of uncertainty and new risks. They provide some practical guidance.

Recent financial crime reforms

The failure to prevent fraud (FTPF) offence

The FTPF is a strict liability offence that applies where a "large organisation" (including most UK financial services firms) fails to prevent criminal fraud that is intended to benefit the organisation carried out by an "associated person". There is a lengthy list of offences covered, including fraud by false representation, fraud by failing to disclose information, obtaining services dishonestly and false accounting. The definition of associated persons is also broadly defined and the intention to benefit covers both indirect and direct benefits and benefits for the defendant and its client. The organisation can rely on a defence if it is able to establish that "reasonable prevention procedures", designed to prevent the fraudulent activity, were in place, or it was not reasonable to have such procedures in the circumstances. On 6 November 2024, the government published final guidance (Guidance) on the FTPF. The new provisions will enter into force on 1 September 2025.

Extended attribution doctrine

The Economic Crime and Corporate Transparency Act (ECCTA) also provides that the actions of a wider remit of senior executives can be attributed to an organisation for the purposes of establishing criminal liability for certain economic crimes. Provisions implementing this expanded liability are currently in force. Previously (except in select circumstances), an organisation could only be criminally liable for misconduct committed by a limited range of individuals who could be identified as its directing mind and will. It is now clear that the misconduct of a larger class of senior representatives can be attributed to an organisation; specifically, an organisation will be guilty of an offence where a "senior manager … acting within the actual or apparent scope of their authority commits a relevant offence". "Senior manager" is widely defined to include those involved in significant decision-making or management of the whole of the organisation or of a part of it. On 25 February 2025, the Home Office also introduced a Crime and Policing Bill that will apply the extended attribution doctrine to all criminal offences in England and Wales (rather than only certain economic offences as currently).

The reforms have been designed to prevent the repeat of high-profile collapses of corporate prosecutions partly due to difficulties establishing that the actions of senior management could be attributed to a business. This came under the public attention during the aftermath of the global financial crisis. The reforms therefore create a new area of risk for firms, which may now face additional criminal liability for the actions of a broad class of senior managers.

KEY POINTS

- Two corporate crime reforms have recently been confirmed and implement important changes for financial institutions: the introduction of a failure to prevent fraud offence and the extension of the attribution doctrine to hold firms liable for a wider range of misconduct by senior managers.
- There are several areas of uncertainty in relation to the scope of the measures, but guidance can be gleaned from recent developments.
- The main areas of risks for firms are the new additional criminal liability that can attach to regulatory failings and the extended remit of senior managers for which firms can now be criminally liable.
- The financial services sector will need to adopt new measures to prepare, although there are pre-existing procedures that can be utilised to comply with the changing regulations.

The Guidance

The FTPF offence will not apply if there were reasonable procedures in place to prevent fraud. The Explanatory Notes[1] to the ECCTA explains that they are "broadly the same as in the offence of failure to prevent tax evasion", which was introduced several years ago. The reasonable procedures are further elaborated on in the official Guidance, which sets out six general principles that organisations should have in mind when developing fraud prevention procedures, alongside illustrative case studies. These principles are:

1. **Top level commitment**: Senior level engagement is essential, and this includes communicating and endorsing the company's fraud prevention measures, committing resources to this effort, and leading by example in fostering an open culture that empowers staff to speak up if they believe fraud is taking place.
2. **Risk assessment**: This should consider the: (i) opportunity; (ii) motive; and (iii) rationalisation by which associated persons may commit fraud that benefits the organisation or its clients (whether indirectly or directly). This is coined as the "Fraud Triangle" in the Guidance, which contains lists of questions under each heading that may provide a useful starting point for any risk analysis.
3. **Robust but proportionate risk-based prevention procedures**: Measures should aim to reduce the opportunity, motive and means to commit fraud. Most financial institutions should be able to build on existing processes, but additional measures may be required depending on the risk assessment and existing safeguards. Often, simply bolting-on fraud wording to current contractual or policy terms will insufficient.
4. **Due diligence**: Given the broad definition of associated persons (which includes persons who provide services on behalf of the organisation), due diligence of third parties who provide such services is identified as an important element of prevention, as is appropriate due diligence in the M&A context to ensure newly acquired business units are also compliant.
5. **Communication**: Training can help employees understand the steps they can take to spot and prevent fraud, with communications to reinforce why this is important. The Guidance emphasises the need to ensure training is monitored for effectiveness and kept updated, and that training should reference the company's whistleblowing policies and procedures.
6. **Monitoring and review**: There are three identified elements for sufficient monitoring of fraud: (i) detection; (ii) investigation; and (iii) ongoing review/monitoring. An important part of this process is learning from experiences of similar reforms and feedback from the introduction of new fraud prevention procedures.

In collaboration with the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA), UK Finance has published financial services specific guidance on the FTPF (FS Guidance).

[1] https://www.legislation.gov.uk/ukpga/2023/56/notes/division/11/index.htm

Areas of uncertainty and new risks

There are several areas of uncertainty on the scope of the FTPF, as well as additional areas of potential liability, including the extraterritorial reach of the offence and the extent to which firms will be liable for associated persons.

Associated persons

The Guidance explains that third parties are an associated person when providing services on behalf of the firm. Third parties do not have to be in a contractual relationship with the firm including where the services are completed as part of a supply chain for the business but there is no direct contractual relationship.

The FS Guidance explains that relevant services could include a wide range of activity that is frequently contracted out by financial institutions; including customer relationship management; payment services; sales and distribution services; advisory services; and brokerage services. The provision of products by associated parties may also be covered by the offence, which includes:

- providing lending facilities or receivable financing;
- providing letters of credit or other forms of trade finance;
- providing access for customers to the firm's own technology products/ platforms; and
- providing and/or underwriting insurance policies or investment products.

The Home Office Guidance provides an example of a bank using another bank for clearing services where the clearing bank (corporately, with the knowledge and involvement of its senior management) commits a fraud offence. The clearing bank would be an associated person of the contracting bank and could be liable for the offence unless a court decides that it had reasonable procedures in place to prevent the fraud.

In short, a wide range of activities and product provision will be covered by the offence therefore firms will need to complete a wholesale assessment of risks created by all third-party relationships. Additional due diligence, auditing and contractual arrangements may all be required to ensure there is sufficient oversight of third parties providing services for firms.

Territorial reach

Proceedings could be issued against a financial institution irrespective of where the organisation is incorporated. In that, the FTPF will be triggered where an associated person commits fraud under UK law or targets UK victims, even if the associated person is based overseas. The FS Guidance addresses common structures for global banks that typically use branches instead of subsidiary structures. The position is complex, but in short, a fraud offence committed by or intended to benefit a branch of a bank headquartered outside the UK could be in-scope of the FTPF offence where there is a sufficient UK nexus. Whereas a fraud offence committed entirely outside the UK by another part of the bank's non-UK legal entity (and which is not intended to benefit the branch) that would likely not have a UK nexus.

Given this, firms should carefully assess the extent to which activities are conducted in the UK, target UK consumers and/or result in loss/profits in the UK. This will be an important part of initial risk assessments, which should form the basis for proportionate prevention procedures (see further below). This is a further area of potentially expanded liability for banks because of the broad potential territorial reach of the offence.

Application in practice

There will be difficulties establishing whether actions are sufficiently egregious to trigger criminal liability because of the inherent problem of proving a dishonest intention as opposed to negligence, as well as the necessary intention to benefit the firm. The guidance material provides case studies that aim to address uncertainty. The 20 illustrations in the FS Guidance include assessment of the following:

- Using a third party to perform services such as customer onboarding, vetting and due diligence services where the service is performed fraudulently.
- Using an intermediary to provide advice services when the intermediary commits fraud.
- Confirming and account settling activities undertaken by UK-based staff for non-UK transactions.
- Arranging loan finance by employees based on false representations.
- Providing retail services by employees on standard terms (such as mortgages, saving accounts and personal loans), which is identified as a low-risk area.

As evident from the types of conduct that may be covered, the fact patterns that could give rise to criminal offences will likely be similar to those that could lead to enforcement action for regulatory failings in many instances; the crucial difference will typically be evidence of the required dishonest intention and intention to benefit. For example, an employee carelessly advising a customer that a financial product has certain risk characteristics, where it does not, would not be a criminal offence, whilst an employee deliberately advising a customer that a product has these characteristics with clear and documented awareness that it does not, may trigger criminal liability.

The guidance material considers examples of mis-selling that could trigger criminal liability, which also align with instances where there could be civil enforcement action.

The Home Office Guidance refers to an investment fund provider promoting investment in a "sustainable" timber company, knowing that, in fact, this company's environmental credentials are fabricated, and that the timber is harvested from protected forest. Investors are deceived into placing funds with the investment fund provider. The base fraud is fraud by false representation. The intent is to benefit the fund provider. As a result, the investment fund provider could be liable unless a court determines that it had reasonable procedures in place to prevent this fraud. The example shows that action that may lead to prosecution will be highly fact specific and requires analysis of the associated person's knowledge and the relevant financial services/product.

Although firms can closely scrutinise internal systems and controls to prevent financial crime, they may have less visibility and control of third-party contractors. As a result, this is a potential risk area that should be reassessed to ensure that there are adequate reasonable prevention procedures in place. The following examples are used in the FS Guidance:

- A firm contracting out the performance of customer on-boarding vetting and due diligence services on behalf of the firm where the firm onboards the third party through its supplier procurement processes and manages the relationship as a supplier relationship.
- An intermediary bank appointed by another bank to provide advisory services on the bank's behalf to the bank's customers.

There may also be fact patterns where the conduct may not amount to regulatory breaches, but the misconduct may fall within the scope of the FTPF. This could potentially arise in relation to outsourcing of services that do not affect the firm's ability to remain authorised but may result in associated persons committing fraud when providing those services for the firm. For example, purchases of IT equipment, certain IT services, building maintenance and the use of non-ICT providers. The recent regulatory requirements in these areas have typically focused on operational resilience as opposed to ensuring financial crime controls. In this respect, the area of critical third parties (CTP), which has only been subject to new regulatory requirements relatively recently, may be an area of high risk for firms, with firms facing challenges ensuring that CTPs, such as technology providers and non-ICT providers (eg cash distribution service providers), are adequately complying with regulatory expectations. Even where there are contractual requirements on third parties to prevent fraud, that may be insufficient to show adequate reasonable prevention measures have been undertaken; the question will be one of reasonableness and proportionality in light of the potential risk of fraud.

The guidance material shows that there will inevitably be complex questions of interpretation and application as to how the offence should be interpreted, taking into account the relevant organisation and the factual matrix. The analysis also illustrates how wide ranging the FTPF offence may be, underscoring the need to evaluate reasonable prevention measures in a comprehensive way, rather than simply relying on existing systems and controls aimed at complying with money laundering or similar financial crime regulations.

Prosecution

The criminal prosecution of a leading bank for anti-money laundering failings illustrates that the FCA is willing to use its criminal powers where necessary to hold firms accountable. However, the financial services regulators have been under increasing pressure recently to adopt a more business-friendly approach. Recent statements from government also suggest that the offence looks to incentivise proactive and pre-emptive steps by corporations to foster a culture of zero-tolerance to criminal activity, as opposed to envisaging an uptick in criminal prosecutions as a result of failings. Given this context, we do not expect to see an immediate marked increase in prosecutions in the area, although there will likely be additional investigations into corporate fraud as the reforms are implemented.

Senior management accountability

An organisation facing liability for the FTPF offence may also face prosecution for the underlying fraud offence if the actions of the relevant associated person can be attributed to the firm. This risk has recently increased because of the extension of the attribution doctrine to a wider range of senior management. The reforms echo the introduction of the Senior Management and Certification Regime (SM&CR) in making it clear that senior managers are accountable for all aspects of the business. In many cases, where a senior manager under the SM&CR is involved in fraud it may trigger liability for the financial institutions for the purposes of the extended attribution doctrine. Nonetheless, each fact matrix will be specific to the situation and particular offence that arises. In addition, it should be noted that each of the regimes have very different objectives. SM&CR looks to hold senior managers individually accountable. On the other hand, the extended attribution doctrine focuses on holding financial institutions liable for actions of senior managers. Given the differences between the two regimes, financial services firms cannot assume that ensuring senior managers comply with the SM&CR will be sufficient to address the new risks arising under the ECCTA.

Practical guidance

For both categories of reform, organisations should be undertaking appropriate risk assessments and re-evaluating procedures in light of the changing enforcement and prosecution landscape. We provide suggestions for preparing for the measures in the following section.

Risk assessment

The first step for firms is assessing the nature and extent of exposure to the risk of those who act in the capacity of an associated person and senior manager. Areas of potential exposure to fraudulent activity include public statements (especially those that might influence investors or customers), representations to counterparties (eg in a trading context) and/or stakeholder groups, and instances where an organisation has obligations to disclose (eg Suspicious Activity Reports). There are strict requirements that apply to many firms for the outsourcing of critical functions that can be usefully utilised to address liability for third parties. The requirements include agreeing contractual frameworks with CTPs, preparing business continuity plans in the case of disruption and planning exit policies to remove a CTP to ensure an adequate crisis response where necessary. Incorporating fraud prevention into these steps required for outsourcing can help to use existing safeguards to contribute to fraud prevention measures for a defence to the FTPF.

Proportionate prevention procedures

Financial institutions should subsequently adopt reasonable prevention procedures to tackle the identified risks. The areas identified as posing the highest level of fraud risk should be assessed first via an exercise of balancing the cost and time of prevention against the likelihood of the risk. For groups that are based or headquartered in the UK with subsidiaries located elsewhere, the Guidance states that a firm might tackle fraud prevention by implementing group level policies or training and nominating a particular person to be responsible for fraud prevention in each subsidiary.

Financial services firms comply with a range of regulatory requirements for authorisation, which can be used as a basis for reasonable fraud prevention procedures. First and foremost, the Systems and Controls Financial Crime Risk framework can be adapted to fulfil the new requirements related to the FTPF. Whilst many of the FCA's rules on financial crime focus on addressing money laundering risks and money laundering offences are not covered by the ECCTA, the principles are nonetheless helpful to firms establishing prevention procedures for fraud. The soundness of using existing requirements as a basis for fraud prevention is evident from the FS Guidance providing several examples where procedures relating to existing regulatory requirements may be reasonable for the purposes of the FTPF offence.

Monitor and review

Businesses should monitor and review prevention procedures and refine where necessary. Businesses can review their fraud prevention procedures by:

- examining relevant whistleblowing cases and subsequent action taken;
- examining other financial crime prevention procedures;
- conducting formalised periodic reviews with documented findings;
- working in collaboration with other organisations such as trade bodies and organisations facing similar risks;
- following advice from professional organisations, such as legal or accountancy bodies to provide objective assessments; and
- examining any relevant examples of investigations and/or enforcement action.

It is important to revisit initial steps to prepare for entry into force of the offence.

Outlook

Where there is a successful prosecution for a FTPF offence, an organisation can receive an unlimited fine – considering all the circumstances in deciding the appropriate level for a particular case. Although we may not see a marked increase in enforcement outcomes, we do expect that there will be a significant uptick in investigations by relevant authorities into corporate fraud. Where a firm does face investigation, co-operation should be considered to ensure that further damage is limited. The level and type of co-operation expected is not standardised. While organisations should be aware of the enforcement risk, the FTPF is primarily designed to encourage organisations to take active steps to prevent fraud.

FURTHER READING

- Failure to prevent fraud: making up for failure to prosecute? (2023) 6 JIBFL 397.
- Risk elimination by legislating: the limits of the law and challenges of reality (2023) 5 JIBFL 287.
- Lexis+® UK: Corporate Crime Practical Guidance: Practice Note: Failure to prevent fraud – the offence.

Authors

Piers Reynolds
Partner, London
T +44 20 7716 4111
E piers.reynolds
@freshfields.com

Laura Feldman
Knowledge Lawyer (Barrister), London
T +44 20 7716 4358
E laura.feldman
@freshfields.com

Freshfields.com