Proskauer

Failure to Prevent Fraud Offence – What you should know

Regulatory & Compliance on **July 3, 2025**

On 1 September 2025, the new UK corporate offence of "failure to prevent fraud" will come into force, as introduced under section 199 of the Economic Crime and Corporate Transparency Act 2023 (the "**Act**").

This client alert covers the new offence's aims, scope including extra-territorial reach, defence availability and some key areas of focus for asset managers from the Home Office statutory guidance (the "Guidance"), published on 6 November 2024.

What is the failure to prevend fraud offence trying to achieve?

The new offence is intended to make it easier to hold organisations to account for fraud committed by employees, or other associated persons, which may benefit the organisation, or, in certain circumstances, their clients. The offence will also encourage more organisations to implement or improve prevention procedures, driving a major shift in corporate culture to help prevent fraud.

If prosecuted, an organisation must demonstrate, on the balance of probabilities, that it had reasonable procedures in place to prevent fraud or that it was unreasonable to expect such procedures to avoid being found liable. In this sense, the new offence (and available defence) is similar to the schemes under section 7 of the Bribery Act 2010 (failure to prevent bribery) and sections 45 to 46 of the Criminal Finances Act 2017 (failure to presvent facilitation of tax evasion).

Which fraud offences are covered by the failure to prevent fraud offence?

The potential offences which can form the "base fraud offence" (the fraud to be prevented) are detailed below and range from offences found in the Fraud Act 2006, common law, the Companies Act 2006 and the Theft Act 1968:

Offence List

1. Fraud by false representation

2. Fraud by failing to disclose information
3. Fraud by abuse of position
4. Participating in fraudulent business
5. Obtaining services dishonestly
6. Cheating the public revenue
7. False accounting
8. False statements by company directors
9. Fraudulent trading

What if we are outside the UK?

The failure to prevent offence applies only where the underlying fraud offence has a **UK connection** or **nexus**.

An offence will fall within this scope if **either** of the following conditions is met:

- at least **one element of the fraudulent conduct** took place in the UK: or
- the **gain or loss** resulting from the fraud occurred in the UK.

This means that if a UK-based employee commits fraud, the employing organisation may be prosecuted and held liable regardless of where it is established.

Who is caught by the new offence?

In contrast to the equivalent offences created by the Bribery or Criminal Finance Acts (which apply to all organisations), entities in scope under section 199 of the Act are large organisations. The offence applies regardless of how organisations are incorporated and could even include partnerships which are not bodies corporate, such as limited partnerships and applies across all sectors of the economy. The Home Office also encourages even smaller organisations outside the formal scope of the offence to review the Guidance as best practice.

Breaking this down, it covers “large organisations”, defined as meeting **two out of three** of the following criteria, as found in the prior financial year to the base fraud offence:

- more than 250 employees.

- more than £36 million turnover.
- more than £18 million in total assets.

It is important to recognise that a relevant base fraud offence can be committed by a "**person associated with the relevant body**". This includes individuals or entities who perform services for or on behalf of the organisation while acting in that capacity, such as employees, agents, contractors, subsidiaries and partners in a partnership. In further detail:

- An employee, agent or subsidiary of a relevant organisation is automatically considered an "associated person" for the purposes of the offence.
- A subsidiary undertaking of a large organisation is considered an associated person for the purposes of the failure to prevent fraud offence. This means that:
    - a parent company can be held criminally liable if a subsidiary commits a fraud that is intended to benefit the parent organisation; and
    - liability may also arise if the fraud benefits a client of the parent company, where the subsidiary provides services for or on behalf of the parent.
- Employees of the subsidiary can bring both the subsidiary and the parent company into scope, as the subsidiary itself can be prosecuted if one of its employees commits a fraud intended to benefit the subsidiary, or the parent company.
- The Guidance clarifies that individuals or firms providing services to an organisation, such as external lawyers, valuers, accountants or engineers, are generally not considered associated persons as they are not acting "for or on behalf of" the organisation.

Importantly, as a **corporate offence only**, **directors and senior managers are not personally liable** for a failure to prevent fraud within the organisation. However, any associated person who commits the underlying fraud offence may still be individually prosecuted for that offence as outlined in the relevant offence list above.

As well as triggering corporate liability for a failure to prevent fraud, an organisation may also be held liable for the base offence, for example if a partner commits a fraud offence in the course of the partnership's business, the partnership itself may also be held criminally liable for the substantive offence.

Does an organisation need to receive a benefit?

An organisation does not need to receive a benefit for the offence to apply. The offence can be triggered as soon as the underlying fraud is committed, even if no gain has yet been, or would ever be, realised. It is sufficient that the fraud was carried out with the intention of benefitting the organisation.

The intention to benefit the organisation does not have to be the sole or dominant motivation of the fraud either. For example, an employee could be setting out to benefit themselves only, but their actions will indirectly benefit the organisation as well. The benefit may also be financial or non-financial (such as an unfair business advantage).

Is there a defence?

Organisations will have a defence if they can show that they have 'reasonable procedures' in place to prevent fraud. Alternatively, if the organisation can demonstrate to the satisfaction of the court that it was not reasonable in all the circumstances, to expect the organisation to have any prevention procedures in place, then this can also qualify as a defence.

What are reasonable fraud prevention procedures?

The Guidance gives examples of reasonable fraud prevention procedures, but notes that the onus will remain on the relevant organisation, where it seeks to rely on the defence, to prove that it had reasonable prevention procedures in place (or that it was unreasonable to expect it to have such procedures). The standard of proof is on the balance of probabilities and the court will determine the question on a case-by-case basis, in light of the specific context, facts and circumstances.

The Guidance advises that the fraud prevention measures put in place should be designed and implemented with the organisation's structure and the territoriality of the offence in mind. The reasonableness of procedures should take account of the level of control, proximity and supervision the organisation is able to exercise over a particular person acting on its behalf.

The procedures must be built around six key principles, set out below, which echo those in the Home Office guidance under the Bribery Act 2010, although in relation to the failure to prevent fraud offence, the need for top-level commitment is addressed first in the relevant guidance, as opposed to proportionality as in the bribery related guidance. While there is no formal priority of principles, this emphasis may well reveal future regulatory focus when applying the new Act.

The Guidance

Principle: Top Level Commitment

Action: Senior management, specifically those charged with governance of the organisation, is expected to demonstrate active and visible leadership in fraud prevention. This can be achieved through:

- Communication and endorsement of the organisation's stance on preventing fraud, including mission statements.
- Ensuring that there is clear governance across the organisation in respect of the fraud prevention framework.
- Commitment to training and resourcing.
- Leading by example and fostering an open culture, where staff feel empowered to speak up if they encounter fraudulent practices.

Principle: Risk Assessment

Action: Risk assessments will be key to identifying any potential areas within the organisation that could be exposed to fraudulent activity and should be reviewed every two years as a minimum.

Assessing those who qualify as "associated persons" for the purpose of the offence provides a good foundation to identify the three elements that could lead to fraudulent activity:

1. Opportunity
2. Motive
3. Rationalisation (that is, opportunity or culture to excuse or justify)

Reviewing internal data analytics, audits, sector specific information and any regulated enforcement action are also key to risk assessing. Testing of risks in emergency scenarios and having a classification of risks by its likelihood and impact are also detailed in the Guidance.

Principle: Proportionate risk-based fraud prevention procedures

Action: It is essential that fraud prevention procedures are tailored to the specific risks and structure of your organisation. These procedures should be risk-based and proportionate, reflecting the degree of control and oversight the organisation has over individuals acting on its behalf.

Where it is determined that implementing specific measures in response to a particular risk is not reasonable, this decision should be clearly documented, including the name and position of the individual who conducted the review and made the determination.

The Guidance notes that it is not necessary or desirable for organisations to duplicate existing work. Equally, it would not be a suitable defence to state that because the organisation is regulated, its compliance processes under existing regulations would automatically qualify as “reasonable procedures”. A balance must be struck. While existing procedures, for example as regards bribery or tax offences, may therefore be a good starting point, these need to be reviewed with the Act specifically in mind.

An organisation must also consider how to reduce the opportunities for fraud, to reduce the motive for fraud and to put in place consequences for committing fraud. Furthermore, the Guidance sets out that organisations should consider how to reduce the rationalisation of fraudulent behaviour, where over time, “one-off” frauds may become normalised as people rationalise certain behaviours, such as other businesses also acting a certain way.

Testing is also identified as a means to evaluate the effectiveness of the fraud prevention measures.

Principle: Due Diligence

Action: Relevant due diligence should be conducted on any “associated persons”, which could include third-party risk management tools, professional regulated status, vetting checks and review of contracts for agents.

Principle: Communication

Action: A strong, visible endorsement of fraud prevention policies is essential for setting the tone across the organisation. This should be supported by tailored training, with attendance records maintained. There should be a culture that promotes openness and transparency, encouraging staff to report any suspected fraudulent activity, including through appropriate whistleblowing processes. Together, these measures strengthen the organisation's ability to detect and respond to fraud risks effectively.

Principle: Monitoring and Review

Action: Regular monitoring of financial controls, tracking attendance at fraud prevention training, updating internal procedures and periodically reviewing contracts with associated persons all help organisations proactively identify and address emerging fraud risks.

What if we are sanctioned?

On conviction, the organisation may be fined (and there is of course likely to be reputational damage also). There may also be resulting civil liabilities, contractual implications, or consequences under procurement regimes. .

For the associated persons who committed the underlying fraud offence, they could be personally prosecuted, which could result in fines, criminal records or a custodial sentence, depending on the offence and its severity.

What are some examples relevant for asset managers?

Asset manager must of course consider their own businesses and that of portfolio companies.

Two examples are provided in the Guidance in relation to investments:

- Example 1: A large company is seeking investments. The accounting department deliberately manipulates the accounts to over-state the profits. The intent of the fraud is to benefit the company by making it appear more attractive to investors. The base fraud here is fraud by false accounting and the associated person is the relevant employee (or employees) in the accounts department. The company could be prosecuted under section 199(1)(a) of the Act and could be liable for failure to prevent fraud, unless the court determines that it had reasonable procedures in

place to prevent such a fraud. Note that the offence applies even if potential investment is not actually secured. It is enough that the fraud was intended to benefit the company.

- Example 2: An investment fund provider promotes 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 fraud by false representation. The intent is to benefit the fund provider. The associated person is the relevant member of staff at the investment fund provider who knowingly used the false information in the investment fund's brochures for clients. The investment fund provider could be liable under section 199(1)(a) of the Act unless a court determines that it had reasonable procedures in place to prevent this fraud. Again, the offence applies even if the investment is not actually secured. It is enough that the fraud was intended to benefit the investment fund provider.

For further information on the failure to prevent fraud offence, please reach out to ukreg@proskauer.com.

View original.

Related Professionals

- **John Verwey**
  Partner
- **Dorothy Murray**
  Partner
- **Michael Singh**
  Associate
- **Rachel E. Lowe**
  Special Regulatory Counsel
- **Sulaiman I. Malik**
  Associate