Browne Jacobson

Navigating the new 'failure to prevent fraud' offence: What organisations need to know

13 December 2024

Government guidance on the new failure to prevent fraud (**FTPF**) offence was published on 6 November 2024. This confirms the offence will come into force on 1 September 2025 - giving in-scope organisations just over nine months to review their fraud risk and implement any enhanced compliance procedures as part of internal governance.

What is the FTPF offence?

The strict liability FTPF offence was introduced as part of the Economic Crime and Corporate Transparency Act 2023 (**ECCTA**) and makes large organisations (as defined below) criminally liable for fraud committed by employees and associates.

The FTPF offence is committed if an "associate" (such as an employee, agent or person performing services for or on behalf of the organisation) commits a specified fraud offence with the intention of benefitting the organisation or its customers/clients. Specified offences include false accounting, fraudulent trading and cheating the public revenue. A guilty organisation is liable to an unlimited fine.

Who does the FTPF offence apply to?

The FTPF offence applies to large organisations that meet two of the three following criteria:

- more than 250 employees;
- a turnover of more than £36 million; and/or
- assets of more than £18 million (**organisation(s)**).

Whilst it is easy to see how large corporates incorporated under the Companies Act 2006 could meet the criteria, it is worth noting that other incorporated bodies may also be caught – such as charities, limited liability partnerships, or other entities incorporated by statute or Royal Charter. Those organisations may also be in scope and should consider whether to act now to mitigate their risk.

Whilst smaller organisations are outside scope for now, this could change in future. Smaller organisations may be expected to improve fraud prevention procedures by the larger organisations they contract with or may have to do so to be successful in tenders.

Reasonable procedures defence

FTPF is the third corporate "failure to prevent" offence in the UK, following established offences of failure to prevent bribery (section 7, Bribery Act 2010) and failure to prevent the facilitation of UK/foreign tax evasion (sections 45/46, Criminal Finances Act 2017).

In-scope organisations have a defence if they can demonstrate that either; i) reasonable procedures were in place to prevent fraud, or ii) it was not reasonable in all the circumstances to expect the organisation to have prevention procedures in place. The burden in i) will be on the organisation to prove that, on the balance of probabilities, it had reasonable procedures in place to prevent the fraud at the point it was committed.

To assist organisations, the Home Office has published guidance on the new offence. The guidance sets out six principles to which organisations should have regard when putting in place fraud prevention frameworks. Organisations will be familiar with the principles as they apply to the two existing failure to prevent offences set out above.

Whilst departure from suggested procedures will not automatically mean an organisation cannot demonstrate reasonable prevention procedures, any such organisation will be required to show how and why the procedures it did have were equivalent or better in the circumstances. Importantly, the guidance expressly states that a failure to conduct a risk assessment will rarely be considered reasonable. This gives in-scope organisations a clear warning that drafting a FTPF policy without first assessing the applicable risks and tailoring the policy to address those risks will be insufficient to establish the defence.

The six principles are:

Top level commitment

Prevention of fraud should come from the top down. The board of directors, partners and senior managers should be committed to preventing fraud and must lead by example. This involves fostering an organisational culture in which fraud is never acceptable and the whole ethos of the organisation demonstrating this at every level, through actions not just words.

As a first step, organisations should consider their culture, what the awareness level/attitude to fraud is and whether steps need to be taken to drive a cultural shift. It may be prudent to consider an audit or cultural review to assess the “as is”, which can then inform the steps the organisation should take to get to the “would like to be”.

Risk assessment

Conducting a risk assessment is a must. Organisations need to assess the nature and extent of exposure to the risk of employees, agents and other associated persons committing the specified fraud offences. The risk assessment should be documented and kept under regular review (annually or bi-annually).

Where organisations already undertake a range of fraud-related risk assessments, it may be effective to extend these to take account of the risks identified within the new offence. Any risk assessment should include the risk of fraud occurring during emergencies when the risk level may be increased due to the circumstances.

Proportionate risk-based fraud prevention procedures

An organisation’s procedures to prevent fraud should be proportionate to the risks faced. Many organisations (particularly those who are regulated) will already have anti-fraud procedures in place. These may be adequate in relation to the new FTPF offence or capable of being built upon to ensure adequacy. The guidance also suggests that the prevention plan should be stress tested by members of the organisation who weren’t involved in designing it. This should be documented and retained.

It would also be prudent to consider reducing the opportunities for fraud, including during the recruitment process by ensuring pre-employment and vetting checks are carried out (including ongoing checks for high-risk roles). Consideration should also be given to whether conflict of interest procedures are robust. Equally, does the organisations bonus structure or working practice encourage risk taking or corner cutting? Are the consequences for committing fraud robust and communicated to staff? If the answer to any of these questions is “no” measures should be taken to address this to mitigate against the risk of fraud being committed.

Due diligence

Organisations should apply due diligence procedures (again proportionate to the risk) on those who perform or will perform services for or on behalf of the organisation. This may include appropriate internet searches or vetting checks. Monitoring staff wellbeing, central to an organisation’s duty of care, may also assist in identifying those more likely to commit fraud because of stress, targets or workload, allowing support can be put in place to prevent that before it happens.

Communication

Good communication is key. Staff and associated persons should be made aware of the organisations prevention policies and procedures. Individuals should be informed about how to raise concerns (including through the organisations whistleblowing procedure) and what steps will be taken by the organisation to investigate. Equally, the consequences for those found to be in breach should be made clear to individuals. This should be achieved by regular communication and training, which should be refreshed at regular intervals so that it doesn’t become stale.

Policies and training should be kept alive in the workplace so that they become part of the culture (again, it's actions not words). Organisations' behavioural standards could be linked to an individual's performance/objectives (especially in the case of managers, leaders and high-risk roles). Equally, the organisation should foster a "speak up" culture and ensure that, where concerns are raised, they are adequately investigated in a timely manner and appropriate feedback given (having regard to any confidentiality obligations).

Monitoring and review

Organisations should continuously monitor and reviews its fraud detection and prevention procedures and make improvements where necessary. This includes learning from investigations and whistleblowing incidents and taking steps to sure up any areas of weakness which may have been identified. Organisations should also decide who will be the "gatekeeper" responsible for ensuring that the necessary reviews happen, are documented and any learnings implemented. The guidance suggests it would be prudent for organisations to review information from its own sector, and action as necessary.

Conclusion

The new FTPF offence comes into effect in nine months' time. Organisations must consider now whether they are in scope of the new rules and, if so, what steps they need to take prior to 1 September 2025 to prepare. Organisations remaining out of scope for now may also find this a prudent time to reflect on and, where necessary make improvements to, fraud prevention procedures.

We can help your organisation:

- Identify "associated persons" and prepare a thorough risk assessment to identify vulnerabilities to fraud from the persons identified;
- Review existing policies and guidance, and update or replace them with new versions, tailored to government guidance, with clear prohibitions on fraud;
- Provide accessible and relevant training on the new offence particularly to those in higher risk positions;
- Check that agreements with agents, distributors, and other third parties contain appropriate contractual terms around fraud; and
- Ensure the anti-fraud tone is set from the top, and regularly reviewed.

If you would like to discuss how we can help, please do get in touch.

Key contact

Helen Simm

Partner

Helen.Simm@brownejacobson.com

+44 (0)330 045 2652

Related expertise

Commercial law

Corporate

Criminal compliance and regulatory

Employment

Financial services regulation

Fraud and asset recovery