GT GreenbergTraurig

# Alert | White Collar Defense & Investigations

November 2024

# UK Failure to Prevent Fraud Offence Widens Net for Corporate Criminal Liability

**Go-To Guide:**

- New "failure to prevent fraud" offense takes effect 1 September 2025 in the UK, exposing large organisations to criminal liability for fraud committed by associates.
- Organisations can implement "reasonable procedures" to mitigate fraud within the organisation, based on six principles outlined in UK government Guidance.
- Senior leadership to drive anti-fraud efforts, including risk assessments, due diligence, training, and whistleblowing processes.
- Organisations should consider reviewing existing policies, allocating resources, and developing fraud prevention measures tailored to their specific risks.

On 6 November 2024, the UK government published its long-awaited Guidance for the new offence of failure to prevent fraud (FTP Fraud Offence), which will come into force on 1 September 2025. The FTP Fraud Offence was introduced via the Economic Crime and Corporate Transparency Act 2023 (ECCTA) and represents the latest tool in UK law-enforcement armoury as part of the government's continuing efforts to improve fraud prevention procedures and establish an anti-fraud culture within UK business

activities. The UK's Serious Fraud Office has stated that it is "*looking forward to using it to penalise large organisations who should be doing better*".[1]

The FTP Fraud Offence is expected to mirror the significant overhaul in corporate compliance that the UK Bribery Act 2010 introduced, and qualifying "large" organisations[2] that do not already have reasonable anti-fraud procedures in place have 10 months in which to implement them. The Guidance, while not binding, provides some non-exhaustive detail about the procedures that large organisations can consider to help mitigate associated persons from committing fraudulent offences.

## The FTP Fraud Offence

The new offence will expose large organisations to criminal liability where an associated person commits a specified fraud offence with the intention of benefitting (directly or indirectly)[3] the organisation or its clients. The offence is effectively one of strict liability, as the organisation is not required to have been aware of the fraudulent activity, albeit it is subject to the statutory defence (see below) of having in place "reasonable" prevention procedures.

The term "associated person" includes employees, agents, subsidiaries, and any other person who performs services for or on behalf of a company or its subsidiaries; a parent company can therefore be held liable for fraud committed by a subsidiary's employee. While the associated person does not need to be convicted of the substantive fraud offence, the prosecution must prove, beyond a reasonable doubt, that the associated person committed the offence before the organisation can be convicted.

## Defence

Organisations can defend themselves by proving they have reasonable procedures in place to prevent fraud, or that it was not reasonable in the circumstances to expect the organisation to have any prevention procedures in place. The Guidance does not define what "reasonable procedures" are, nor does it provide a list for organisations to follow. Whether "reasonable procedures" are in place will be assessed on a case-by-case basis, taking into account the relevant circumstances and facts surrounding the alleged misconduct.[4] The burden, however, will be on the organisation to prove that it had reasonable procedures in place to prevent fraud at the time that fraud was committed.

## Reasonable Fraud Prevention Procedures

Similar to the Ministry of Justice's guidance on the UK Bribery Act 2010, the Guidance sets out six principles which an organisation should consider when designing, implementing, and maintaining a fraud prevention framework, including enabling direct access to an organisation's board and CEO and ensuring a reasonable and proportionate budget is designated to implement a reasonable fraud prevention plan. The six principles include:

1. Embedding a top-level commitment to fraud prevention.

[1] Global Investigations Review, "Senior SFO lawyer: failure to prevent fraud heralds an 'exciting time' for the agency," 13 September 2024 (subscription required).
[2] Namely organisations which meet at least two of the following conditions for the financial year preceding the year of the alleged fraud offence: (i) a turnover of more than £36 million; (ii) more than £18 million in total assets; and/or (iii) more than 250 employees: section 201 ECCTA.
[3] Section 199(1) and (2) ECCTA. Notably, the definition of "*benefit*" under ECCTA is wider than the UK Bribery Act 2010 definition.
[4] Chapter 2.6 of the Guidance.

2. Conducting dynamic, documented, and regular risk assessments.
3. Ensuring procedures are proportionate to the fraud risks the organisation faces.
4. Taking a risk-based approach to service provider due diligence.
5. Communicating fraud prevention measures internally and externally, including through training and developing whistleblowing mechanisms.
6. Regularly monitoring and reviewing procedures' effectiveness.

The Guidance expects senior management to take the lead, clearly communicating the organisation's policies and procedures, as well as fostering a culture in which employees feel able to report potential cases of fraud via a robust whistleblowing process. The Guidance is explicit regarding the necessity for risk assessments to inform any policy and procedure implemented and that such policies and procedures are subject to regular reviews; *"…it will rarely be considered reasonable not to have even conducted a risk assessment…"*[5] The Guidance highlights, however, that organisations may consider it more effective to extend existing assessments.

Based on an organisation's risk assessment results, reasonable fraud prevention procedures – including appropriate due diligence procedures – should be proportionate to the risks identified and aimed at reducing the opportunity and motive to commit fraud. The Guidance stresses that such reasonable procedures should be put in place as quickly as reasonably possible. The Guidance also places particular emphasis on training, stating that "*training and maintaining training are key*."[6]

Depending on the organisation's structure, parent organisations should also consider how to prevent their subsidiaries from committing fraud, such as by implementing group-level policies or training and ensuring that there is a nominated person responsible for fraud prevention in each subsidiary. Non-UK organisations should also consider whether it is appropriate for them to adopt group-wide policies, depending on whether their activities may give rise to a risk of fraud taking place in the UK.

## Takeaways

With 1 September 2025 confirmed as the FTP Fraud Offence effective date, the stage is set for enforcement to begin.

Organisations should consider taking the following steps now in preparation for the FTP Fraud Offence:

- Allocate appropriate resources and corporate governance to manage fraud prevention on the organisation's behalf and maintain clear communication of the organisation's stance on fraud.
- Undertake an appropriate risk assessment to identify potential areas of risk.
- Review existing policies and procedures and consider whether they need to be updated in anticipation of the FTP Fraud Offence.
- Consider internal control systems and due diligence.

[5] Chapter 2.6 of the Guidance.
[6] Chapter 3.5 of the Guidance.

- Review and deliver appropriate training to employees and agents and ensure awareness of whistleblowing procedures.
- Maintain regular monitoring and review of fraud-related risks.

Individual sectors may also choose to develop specific guidance on the preventative measures organisations can take in response to their industry's particular risks. Such guidance would be advisory only, and where it conflicts with the Guidance, the latter will take priority.[7]

Organisations should familiarise themselves with the Guidance and the FTP Fraud Offence before implementing preventative measures.

## Authors

This GT Alert was prepared by:


- Rebecca Meads | +44 (0) 203.349.8700 | Rebecca.Meads@gtlaw.com
- Alex Swan | +44 (0) 203.349.8700 | Alex.Swan@gtlaw.com
- Greta Barkle ǂ | +44 (0) 203.349.8700 | Greta.Barkle@gtlaw.com
- Gavin Costelloe | +44 (0) 203.349.8700 | Gavin.Costelloe@gtlaw.com
- Helen Sotillo | +44 (0) 203.100.6707 | Helen.Sotillo@gtlaw.com
- Christina Papanastasiou ˇ | +44 (0) 203.349.8700 | Christina.Papanastasiou@gtlaw.com

ǂ *Admitted in New Zealand. Not qualified in England and Wales.*

ˇ *Not admitted to the practice of law.*




[7] Chapter 1.4 of the Guidance.