

White Collar Defense and Investigations



November 14, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Andrew M. Good

Partner / London
44.20.7519.7247
andrew.good@skadden.com

Ryan D. Junck

Partner / London
44.20.7519.7006
ryan.junck@skadden.com

Jonathan Benson

Counsel / London
44.20.7519.7218
jonathan.benson@skadden.com

Jason Williamson

European Counsel / London
44.20.7519.7093
jason.williamson@skadden.com

Frank Lech

Trainee Solicitor / London
44.20.7519.7000
franciszek.lech@skadden.com

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

22 Bishopsgate
London EC2N 4BQ
44.20.7519.7000

UK Government Publishes Guidance on the New 'Failure to Prevent Fraud' Offence

Introduction

On 6 November 2024, the UK government published its guidance on the new 'failure to prevent fraud' offence, which was introduced in the Economic Crime and Corporate Transparency Act 2023 (ECCTA 2023).¹ We covered the details of the new offence in our 12 September 2024 alert: In summary, the establishment of the new offence will mean that, starting from 1 September 2025, companies can be held criminally liable where a fraud offence is committed by an "associated person" of the company.

The term "associated person" applies to employees, agents, subsidiaries and any persons providing services for or on behalf of the company or the company's subsidiary.² Helpfully, the guidance explains that franchisees or entities within a company's supply chains will not be "associated persons," provided they are not providing services for or on behalf of the relevant body.

Notably, it will be a defence to show that a company had "reasonable fraud prevention" procedures in place at the time of the alleged wrongdoing. The guidance sets out the key considerations for companies implementing reasonable fraud prevention procedures. We review the guidance in more detail below.

Reasonable Fraud Prevention Procedures

The 'failure to prevent fraud' offence is modelled on the two other "failure to prevent" offences already in force in the UK, namely the 'failure to prevent bribery' offence³ and the 'failure to prevent tax evasion' offence.⁴ Those offences include a procedures-related defence that the 'failure to prevent fraud' offence mirrors. A company will be able to avoid criminal liability for failing to prevent fraud where the company can prove that it had "reasonable" fraud prevention procedures in place at the time of the alleged fraud (or that it was reasonable not to have such procedures in place).⁵ The guidance presents the contours of what fraud prevention procedures would be considered "reasonable" if they came under law enforcement scrutiny.

The guidance is based on six key "principles," which mirrors similar guidance issued by the UK government relating to the failure to prevent bribery and tax evasion offences. Those principles are:

¹ Economic Crime and Corporate Transparency Act 2023, Sections 199-206.

² Section 199(9) of the ECCTA 2023 provides that whether or not a particular person provides services for or on behalf of a company "is to be determined by reference to all the relevant circumstances and not merely by reference to the nature of the relationship between that person and the body."

³ Bribery Act 2010, Section 7.

⁴ Criminal Finances Act 2017, Sections 45-46.

⁵ ECCTA 2023, Sections 199(4)-(5).

UK Government Publishes Guidance on the New ‘Failure to Prevent Fraud’ Offence

- i. Top-level commitment.
- ii. Risk assessment.
- iii. Proportionate risk-based prevention procedures.
- iv. Due diligence.
- v. Communication (including training).
- vi. Monitoring and review.

The principles are intended to be flexible and outcome-focused in order to enable adaptation to each in-scope company’s profile and thus ease implementation burden. Since the guidance parallels previous guidance relating to the “failure to prevent bribery” offence, in many cases companies can leverage best anti-bribery practices to implement fraud-prevention procedures.

Top-Level Commitment

The guidance provides that responsibility to prevent and detect fraud rests with those charged with governance of the company. Senior management⁶ is therefore expected to take an active role in preventing fraud and fostering an open culture that empowers employees to report suspected fraud (and other misconduct). The level and nature of senior management’s involvement will depend on the size and structure of the relevant entity, but will likely include:

- Communicating and endorsing the company’s stance on preventing fraud (including the company’s mission statements).
- Ensuring clear governance intended to prevent fraud is in place.
- Demonstrating a commitment to training and resourcing.
- Leading by example and fostering an open culture where staff feel empowered to denounce fraudulent practices.

For example, the guidance emphasises the expectation that the person responsible for overseeing the fraud prevention measures should have direct access to the company’s board or CEO, and that companies should maintain a reasonable and proportionate budget to train staff and implement the company’s fraud prevention plan.

The guidance also sets out the expectation that senior managers will foster an atmosphere that encourages staff to “speak up early if they have any ethical concerns, no matter how minor.” Regulators will consider an effective whistleblower and “speak-up” programme central components to policies and procedures designed to prevent fraud within an organisation. The guidance highlights that companies should establish

“clear governance” of an organisation’s fraud prevention framework, including clear roles and responsibilities, reporting lines and reports to the board.

Risk Assessment

Companies that already undertake risk assessments, for example in relation to economic crime or money laundering, should extend their risk assessments to include the risk of fraud offences that fall within the scope of the new offence.⁷ If a company does not conduct financial crime risk assessments, the company should consider doing so — the guidance makes clear that it will “rarely” be considered reasonable to have not conducted a risk assessment.

Companies can develop types of risk for their assessments by reference to: i) the opportunity; ii) the motive; and iii) the rationalisation of a relevant “associated person” to commit fraud. The risk assessment should be based on information obtained from data analysis, previous audits, sector-specific information, best practice guidelines or toolkits from industry bodies, and relevant enforcement actions. The guidance foresees that future deferred prosecution agreements (see [our December 2020 alert](#) for more about these agreements) related to the offence would also inform companies about potential risks.

Proportionate Risk-Based Fraud Prevention Procedures

Enforcement officials will expect companies to prepare fraud prevention plans that include procedures designed to prevent fraud by associated persons. These procedures should be proportionate to the risks identified at the risk assessment stage, as well as the nature, scale and complexity of the company’s activities. If a company considers that the risk is sufficiently low to justify not introducing specific measures, the company should document this decision and the name and position of the person who authorised it.

While the guidance explicitly states that duplication of existing efforts is not required, compliance with existing regulatory requirements will not automatically constitute “reasonable” fraud prevention procedures within the meaning of the defence. Accordingly, companies should conduct a gap analysis to assess if their existing compliance mechanisms sufficiently address the fraud risks identified in their risk assessments. According to the guidance, companies should consider whether fraud prevention measures should be tested by individuals within the organisation who were not involved in writing the procedure.

⁶ The guidance defines “Senior Manager” by reference to Section 196(4) of the ECCTA 2023: namely an individual who plays a “significant role” in making decisions about “the whole or a substantial part of the activities” of the company or actually manages or organises the whole or a substantial part of the company’s activities.

⁷ In England and Wales, this includes fraud by false representation, fraud by failing to disclose information, fraud by abuse of position, obtaining services dishonestly, false accounting, false statements by company directors, and fraudulent trading and cheating the public revenue.

UK Government Publishes Guidance on the New 'Failure to Prevent Fraud' Offence

Due Diligence

Regulators will expect companies to conduct adequate due diligence on relevant associated persons to mitigate identified risks of fraud. These due diligence procedures should be proportionate to the level of risk. Application of existing due diligence procedures established in relation to other risks (such as financial crime) will not necessarily provide an adequate response to the risk of fraud and should be reviewed.

The guidance sets out best practices in this regard, which include:

- Using appropriate technology such as third-party vendor risk management tools, screening tools, vetting checks and trading history.
- Reviewing contracts to include adequate provisions on observing the company's fraud policies and providing an option to terminate in the event of breach.
- Monitoring the well-being of staff and agents to identify persons at higher risk of committing fraud due to, for example, stress, targets or workload.

Communication and Training

Companies will be expected to train staff on the fraud prevention policies and procedures, including by administering specific fraud-focused training where appropriate. Communication of commitment to prevent fraud should be consistent across all levels of corporate hierarchy. This could be achieved, for instance, by adding language about fraud prevention to existing policies and procedures (for example, in relation to sales targets or customer interactions). Publishing the outcomes of internal fraud investigations and the sanctions imposed are also considered part of the communication on anti-fraud measures.

As noted above, regulators view whistleblowing procedures as central components of an effective fraud prevention policy. Therefore, companies should ensure that staff are familiar with the relevant whistleblowing policies. The UK guidance on whistleblowing for employers offers a repository of good practices.⁸

Monitoring and Review

Companies are expected to monitor and review their fraud detection and prevention procedures and to update those in response to the gaps identified after they were adopted. Previous internal investigations into fraud incidents, whistleblower reports and sector-specific information should all inform the review of existing policies. The guidance also suggests that technology, including AI, may be useful in detecting fraud.

⁸ Dept. of Business Innovation & Skills, *Whistleblowing Guidance for Employers and Code of Practice* (March 2015).

Further Guidance

What is considered to be a "proportionate" fraud prevention measure will vary between different sectors and risk profiles of the companies in scope of the new offence. The guidance therefore foresees that some industry bodies or sectoral associations will publish sector-specific guidance to set benchmarks or provide further guidance regarding obligations.

However, companies looking to sectoral guidance should ensure that they review the government guidance alongside any sector-specific guidelines. Under the ECCTA 2023, sectoral guidance will be advisory only; companies must therefore ensure that they comply with the legislation and follow the government's guidance closely.

Enforcement

If convicted for failing to prevent fraud, the penalty is a fine. The guidance makes clear that the offence can be prosecuted by the Crown Prosecution Service or the Serious Fraud Office.

Under the guidance, cooperating with law enforcement and making full disclosures will be a factor the agencies weigh when determining whether to bring a prosecution, and if so, whether the case is apposite for a deferred prosecution agreement.⁹ Companies should therefore consider obtaining legal advice promptly after discovering a potential issue.

Takeaways

Following publication of the guidance, the new offence will enter into force on 1 September 2025. As detailed in our previous alert, this is a significant update to the tools available to law enforcement to hold organisations accountable for fraudulent activity. The offence has a broad jurisdictional reach and applies to conduct with a UK nexus even if that offence is undertaken by a company outside of the UK.

Companies should consider using this implementation period to review existing fraud prevention procedures, update risk assessments and training programmes, and assess whether any new procedures are required. This review should be conducted across the corporate group given the jurisdictional reach of the new offence. Organisations should measure their fraud prevention programmes against the guidance to ensure that, by 1 September 2025, they have robust procedures in place that are reasonably designed to prevent fraud and to mitigate the risk posed by the new offence.

⁹ Section 206(3) of ECCTA 2023 adds the new offence of failure to prevent fraud to the list of offences for which deferred prosecution agreements are available under Schedule 17 of the Crime and Courts Act 2013.