FAILURE TO PREVENT FRAUD: A 10 MINUTE GUIDE

The Economic Crime and Corporate Transparency Act 2023. A summary of the relevant guidance to organisations on the offence of failure to prevent fraud

If a fraud is committed in a firm, it brings both moral, reputational and legal risk. Recent developments have rendered all these risks more acute. This article is designed to guide practitioners and organisations through the potential minefield of failure to prevent fraud and the recently published guidance pursuant to it.

Chapter 1. Introduction

The regime is a new one. Section 199 of the Economic Crime and Corporate Transparency Act 2023 ("the Act") created a new criminal offence; the Failure to Prevent Fraud. The Act will come into effect in early August 2025. However, the Home Office Guidance ("the Guidance") was published on 6th November 2024. The Act is broad in scope. It is the Guidance that provides companies and their lawyers with an understanding of the aims and ambit of the offence. The statute aims to make it easier to hold organisations to account for fraudulent behaviour committed by employees or other associated persons where this behaviour benefits the organisation or (in some circumstances) their clients (Home Office Guidance 1.1, para. 4). The secondary aim of the legislation is preventative; it seeks to encourage better fraud prevention procedures and shift corporate culture in doing so (Guidance 1.1, para. 4).

The statute and its accompanying guidance are essential reading for organisations which fall within their scope, and practitioners instructed to represent such organisations. Though it is advisory, a court will evaluate the extent to which an organisation charged with the Failure to Prevent Fraud offence had complied with the Guidance (Guidance 1.2, para. 3). This article will provide a streamlined overview of the offence and on how organisations and legal professionals can prepare to comply.

Chapter 2. Overview of the offence

An organisation will be criminally liable if an employee, agent, subsidiary, or other 'associated person' commits a fraud, in doing so they intend to benefit the relevant organisation, and the organisation did not have reasonable fraud prevention procedures in place. Knowledge or direction on the part of the organisation's senior managers or directors is not a prerequisite (ECCTA 2023, section 199).

Once a prosecution is brought, the burden is on the organisation to prove they have complied with the requirements in the Act on the balance of probabilities (ECCTA 2023, section 199(4)). The offence sits alongside existing law, meaning that where it is in the interests of justice, two separate charges can be brought; firstly, against the person who committed the fraud offence and, secondly, against the organisation which failed to prevent it (Guidance 1.1, para. 3).

2.a. The base fraud offence

The base fraud offence (in England and Wales) comprises acts which amount to, or which aid, abet, counsel or procure the commission of, any offence listed in Schedule 13 of the Economic Crime and Corporate Transparency Act 2023. In England and Wales, these are as follows:

1. Offences in the Fraud Act 2006, section 1
    a. Fraud by false representation (Fraud Act 2006, section 2)
    b. Fraud by failing to disclose information (Fraud Act 2006, section 3)
    c. Fraud by abuse of position (Fraud Act 2006, section 4)
2. Participation in a fraudulent business (Fraud Act 2006, section 9)
3. Obtaining services dishonestly (Fraud Act 2006, section 11)
4. Cheating the public revenue (common law offence)
5. False accounting (Theft Act 1968, section 17,)
6. False statements by company directors (Theft Act 1968, section 19)
7. Fraudulent trading (Companies Act 2006, section 993)

2.b. Types of organisations to which the legislation applies

Any large, incorporated body or and partnership, across any sector of the economy, can commit the Failure to Prevent Fraud offence (ECCTA 2023, section 199(13)). Incorporation may be by any

means (ECCTA 2023, section 199(13)). Bodies incorporated, and partnerships formed, outside the UK may be liable if they have a UK nexus (Criminal Justice Act 1993, sections 1-2).

2.b.i. 'Large'

A large body or partnership is one which meets at least two of the following criteria in the financial year of the organisation that precedes the year of the base fraud offence alleged (ECCTA 2023, section 201):

1. More than 250 employees;
2. More than £36 million turnover; and/or
3. More than £18 million in total assets.

2.b.ii. UK nexus

To be prosecuted under the statute, one of the requisite acts of the base fraud offence must have taken place in the UK, or the actual gain or loss must have occurred in the UK (Criminal Justice Act 1993, sections 1-2).

2.c. Associated persons

An associated person (who would commit the base fraud offence) is an employee or agent of the relevant body, or a person who otherwise performs services for or on behalf of the body (ECCTA 2023, section 199(7)-(9)). The Act does not cover persons providing goods for or on behalf of the organisation. Subsidiaries are associated persons when an undertaking of a large organisation (ECCTA 2023, section 199(7)(a)).

Relevant organisations can be prosecuted if an associated person's conduct *constitutes* the base fraud offence, even if the associated person is *prosecuted* for an alternative offence or is not prosecuted at all (ECCTA 2023, section 199(1)). If the associated person has been convicted of the base fraud offence, this is admissible in proceedings against the organisation for failure to prevent fraud (Guidance 2.2, para. 3). If the organisation is prosecuted but the associated person is not, the burden is on the prosecution to prove to the criminal standard that the identified individual did in fact commit the base fraud offence (Guidance 2.2, para. 4).

2.d 'Intending to benefit'

There is no requirement for the organisation to *in fact* benefit from the fraudulent conduct (Guidance 2.4, para. 2). The benefit need not be financial, for example a business advantage gained by the organisation or a disadvantage experienced by a competitor would be sufficient (Guidance 2.4, para. 6).

Chapter 3. Prosecution and Defences

The offence of failure to prevent this fraud can be prosecuted by (Guidance 2.7.1, para. 2):

1. The Crown Prosecution Service (for England and Wales);
2. The Crown Office and Procurator Fiscal Service (for Scotland);
3. The Public Prosecution Service for Northern Ireland; and
4. The Serious Fraud Office (for England, Wales and Northern Ireland).

There are two available defences available to organisations prosecuted for the offence:

A. The organisation has in place reasonable procedures to prevent fraud, or 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 (ECCTA 2023 sections 199(4) and (5));
B. The relevant organisation is, or was intended to be, the victim of a fraud that was intended to benefit the organisation's clients (ECCTA 2023 section 199(3)).

3.a. Reasonable Procedures to Prevent Fraud

There are five core principles governing whether procedures are reasonable:

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

3.a.i. Top level commitment

The guidance places a strong emphasis on responsibility for the prevention and detection of fraud on those charged with the governance of the organisation (Guidance 3.1, paras. 1-2). It does acknowledge that their role may adapt depending on the size and structure of the relevant body, but that overall, any responsibility is likely to include:

1. Communication, governance and endorsement of the organisation's stance on preventing fraud by, for example, making effective formal statements of (Guidance 3.1.1, paras. 1-2):
    a. A commitment to reject fraud and outline its consequences;
    b. Naming those involved in the development and implementation of the organisation's fraud prevention procedures

2. Commitment to training and resourcing by, for example, (Guidance 3.1.3, para. 1):
    a. Allocating a reasonable and proportionate budget.

The guidance allows for delegation to senior members of staff, such as a 'Head of Ethics and Compliance' (Guidance 3.1.2, para.2).

3.a.ii. Risk assessment

Risk assessments are said to be crucial in identifying where fraud may be committed and allow an organisation to appropriately tailor their prevention procedures (Guidance 3.2, para. 2). If necessary, evidence of a risk assessment can form part of an organisation's defence upon prosecution (Guidance 3.2.5, para. 2 *and* Guidance 3.2.7 para. 2). Risk assessments should be documented and kept under regular review (Guidance 3.2.7, para. 1).

Those charged with governance are expected to incorporate risk assessment into their responsibilities, such as (Guidance 3.1.2, para. 3):

1. Horizon scanning for new fraud risks
2. Approving the assessment of risk
3. Developing and implementing fraud detection measures

The guidance is clear that a court will importantly consider the incorporation of risk assessment *throughout* the organisation and encourages reasonable delegation of risk assessment to

nominated individuals. In substance, any risk assessments should be dynamic, with decisions as to delegation documented and kept under regular review. The Guidance refers to the 'fraud triangle' to help organisations assess what kind of risk assessment is most suitable for them. The three elements of the fraud triangle consist of Opportunity, Motive and Rationalisation:

Opportunity (Guidance 3.2.1, para. 1)

Where, within the organisation, do opportunities for fraud exist? For example, is there a high staff turnover?; Are contractors, for example, operating with minimal oversight?; Are emerging, and perhaps little understood technologies (such as AI) creating new opportunities for fraud?

Motive (Guidance 3.2.2, para. 1)

Does any reward and recognition system incentivise fraud? Are there particular financial or operating pressures on the company? Does the corporate culture disincentivise whistleblowing?

Rationalisation (Guidance 3.2.3, para. 1)

Is the culture of the organisation or sector tolerant of fraud?

The Guidance proceeds on the basis that only through consistent risk assessment can organisations manage the threat of fraud and demonstrate that management to investigators.

The guidance does seek to reassure organisations that not every eventuality can be planned for, and emergency or unforeseen situations will occur. The reassurance, however, is qualified with some detailed guidance on how organisations still can and should plan for the unplanned. Organisations should attempt to scope out possible future emergencies and formalise relevant procedures which will include, in certain cases, provisions for organisations returning 'to normal' once the emergency has passed. Failing to undertake any risk assessment for emergencies may mean that the organisation is not considered to have 'reasonable fraud prevention measures' in place (Guidance 3.3.6, para. 3). We also pause to observe that if a fraud has been committed, investigators and prosecutors are quick to conclude that there was an absence of measures to prevent it.

3.a.iii. Proportionate risk-based fraud prevention procedures

After undertaking a risk assessment, organisations are expected to draw up a fraud prevention plan that is proportionate to the fraud risks it faces and to the nature, scale and complexity of the organisation's activities (Guidance 3.3, paras. 2-3). Measures should be introduced to address each facet of the fraud triangle (Guidance 3.3.1 - 3.3.4).

To ensure a procedure is proportionate to the risk, it should be tested (Guidance 3.3.7, para. 1). It is best practice for staff who were not involved in the writing of the procedures who are tasked with testing them (Guidance 3.3.7, para. 1). While private sector organisations can decide internally how to test their fraud prevention measures, public sector organisations should look to the Government's International Public Sector Fraud Forum guidance.

While it is acknowledged that, in some limited circumstances, it may be reasonable not to introduce measures to address an identified risk, such a decision should be well-documented (Guidance 2.6, para. 8).

3.a.iv. Due diligence

Organisations, especially those facing the greatest fraud risks, are likely already to undertake a variety of due diligence processes. Even so, organisations with a high exposure to risk should evaluate whether their procedures are sufficient under the new guidance and document decisions as to the due diligence procedures undertaken (Guidance 3.4, para. 3).

3.a.v. Communication & Training

There should be a robust communication of anti-fraud policies of the organisation to employees and other associated persons. Where an organisation has a clearly articulated policy against fraud, associated persons will be deterred from committing fraud offences (Guidance 3.5, para. 2). Clearly articulated policies also forge a transparent and ethical corporate culture where fraud is less likely to occur and more likely to be identified (Guidance 3.5, para. 2). In order to be effective, communication should be consistent across all levels of the organisation, and staff at all levels should be equipped with the tools to identify when they and those around them might be at risk of engaging in an illegal act (Guidance 3.5.1, para. 3).

Whistleblowing procedures should be well-known to staff and appropriate to tackle the risks identified in the organisation's risk assessments (Guidance 3.5.2, para. 3). Reporting channels should be independent, responses to reports should be swift, and investigations should be

launched quickly. Best practice would involve the consultation of trade unions or employee representatives before procedures are implemented (Guidance 3.5.2, para. 3).

3.a.vi. Monitoring and review

Organisations should routinely monitor and review their fraud detection, investigation and prevention measures (Guidance 3.6, para. 1). An organisation may conduct its review internally or arrange for an external party to complete the task (Guidance 3.6.2, para. 2).

Relevant organisations can review their fraud detection and prevention procedures by seeking internal feedback from the staff members tasked with reviewing fraud detection analysis, examining any investigations or relevant whistleblowing cases and the subsequent action taken, and working with other organisations (Guidance 3.6.2, para. 3).

3.b. Victimhood

The second defence available to organisations charged with the Failure to Prevent Fraud is to establish that the organisation was, or was intended to be, the victim of a fraud that was intended to benefit the organisation's clients (ECCTA 2023 section 199(3)). An organisation cannot claim that the consequences of being charged with the offence of failure to prevent fraud amount to the organisation being a victim of the fraud (Guidance 2.4, para. 7).

Chapter 4. The offence in practice

The Law Commission paper titled 'Corporate Criminal Liability' (2022) sets out the purpose of the creation of the 'failure to prevent [fraud] offence'. Knowing this helps relevant organisations in preparing for its enforcement. The problem that paper sought to address was the barrier created by the 'identification principle'. In practice, the controlling mind and will of a company with which to "identify" is limited to a small number of directors and senior managers. The paper says, *'concern has been expressed that the identification principle does not adequately deal with misconduct carried out by and on behalf of [large] companies*', making it hard to prosecute said companies. The "failure to prevent" model thus will make it easier to prosecute organisations whose employees are involved in wrongdoing.

The new Failure to Prevent Fraud offence is a concerted effort to prompt a major, preventative shift in corporate culture. The Guidance is clearly directed at changing corporate culture on pain of potential prosecution in the event that any employee misconducts themselves in a proscribed way.

The new offence clearly seeks to address a live issue. Its guidance provides extensive advice on how to prepare large organisations for the task of compliance. The scope for prosecution has undoubtedly widened, but the legislation and guidance both stress the principles of proportionality and reasonableness with reference to any steps an organisation will be required to take. Experience is that those concepts are subjective, and likely to be widely construed by investigators and prosecutors, particularly where there has been demonstrably misconduct by employee or associated persons. Underpinning the statute and woven throughout the Guidance is the core principle that, in implementing the suggestions made, an organisation will be better insulated against liability and, crucially, reduce the likelihood that a fraud offence will be committed by its associated persons.

Further Guidance

It is of note that the new legislation and guidance overlaps with several existing legislative and regulatory regimes. Significant examples of such overlap are the failure to prevent facilitation of tax evasion offence under Criminal Finances Act 2017, existing auditing requirements (Section 475 of the Companies Act 2006, *and* ISA (UK) 240 (Revised May 2021) - The Auditor's responsibilities Relating to Fraud in an Audit of Financial Statement), and the UK Corporate Governance Code (*see* Guidance Chapter 4).

Organisations should be aware that while existing regimes may contain *similar* requirements, the new criminal offence warrants a *full review* of an organisation's fraud prevention procedures. If investigators are involved, organisations would already be starting with the disadvantage that a fraud has, in fact, been committed. Without such a full review of procedures taking account of the Act and Guidance, investigators and prosecutors are unlikely to deem policies reasonable.

Isotta Reichenbach and Emily Griffiths
Pupil Barristers
187 Chambers