

Heralding a new era of corporate accountability

Changes to the rules around failure to prevent fraud have now changed – but to what effect? By Nick Scott, Christopher Coltart KC, Christopher Veal and Richard Edmond

The scope for corporate criminal liability in the United Kingdom has widened significantly after the introduction of a new offence of failing to prevent fraud. The offence was created by the Economic Crime and Corporate Transparency Act 2023 and took effect on 1 September 2025.

Much like the Bribery Act 2010 before it, the new legislation establishes criminal sanctions – in the form of hefty financial penalties – for organisations that fail to take proactive steps to prevent misconduct. Its arrival prompts large firms and their subsidiaries to ask: are our fraud prevention measures robust enough to withstand the scrutiny of the criminal courts?

Application

The offence can be committed in a number of different ways, depending on who commits the fraud offence and the identity of the intended beneficiary.

Large organisations are liable when an ‘associated person’ commits a fraud intending to benefit:

- the organisation itself
- clients of the organisation to whom the associated person provides services on the organisation’s behalf
- subsidiaries of the organisation’s clients where the associated person provides services to those subsidiaries on the organisation’s behalf

These provisions create a broad scope for liability – an associated person is defined as an employee, agent or subsidiary undertaking of the organisation, or a person otherwise performing services on the organisation’s behalf.

Large organisations are also exposed when the employee of its subsidiary commits a fraud intending to benefit the parent organisation.

The subsidiaries of large organisations face liability when the subsidiary’s employees commit fraud intending to benefit the subsidiary.

‘Large organisation’ is defined as an organisation meeting at least two of the following conditions:

- more than 250 employees
- annual turnover in excess of £36 million
- assets above £18 million

Offences within scope

The qualifying fraud offences are:

- Cheating the public revenue
- False accounting
- False statements by company directors
- Fraudulent trading

- Fraud
- Participating in fraudulent business carried on by a sole trader
- Obtaining services dishonestly
- The Scottish common law offences of fraud, uttering and embezzlement

The Act leaves open the possibility of money laundering offences or other comparable fraud offences being added to the list.

Defences

As with offences under the Bribery Act 2010, there is no requirement for directors or senior officers to have been aware of the conduct for the organisation to be liable.

To avoid liability, the organisation must demonstrate either that:

- Reasonable fraud prevention procedures were in place; or
- It was not reasonable to expect the organisation to have fraud prevention procedures in place.

Note further that the organisation will not be liable if it was the intended victim of the offence.

In every case, the prosecution must prove beyond reasonable doubt that the fraud was committed, whether or not there were criminal proceedings against the associated person.

Territorial reach

There must be some link to the United Kingdom either because:

- Some part of the fraudulent conduct occurred in the UK; or
- There was an actual gain or loss in the UK resulting from the fraud.

As such the offence will not apply to organisations in the UK whose employees or subsidiaries have committed fraud overseas, where there was no gain or loss in the UK resulting from the fraud. Conversely, if a UK-based employee commits fraud, his/her employer could be prosecuted wherever they are located.

Home Office guidance

The Act mandates the issue of guidance to assist firms in complying with the legislation, with such guidance issued by the Home Office in November 2024. Chapter 3 of the Guidance sets out six principles to guide the implementation of reasonable fraud prevention measures, which are summarised as follows:

3.1 Top-level commitment: The guidance places responsibility on the board, partners and senior management. They should set a clear tone that fraud is not tolerated, establish and minute governance for prevention and detection, allocate named responsibilities (including risk assessment, investigations, whistleblowing and reporting), ensure the compliance lead has direct access to the board, resource the programme proportionately (including during staff changes), and model expected conduct so that staff feel able to speak up at an early stage.

An example measure would be to appoint a board member as 'fraud prevention champion' with responsibility for oversight and reporting.

3.2 Risk assessment: Firms should undertake a documented assessment of where fraud could be committed by associated persons, mapping the types of associated persons and roles at risk, and analysing opportunity, motive and rationalisation. Those implementing the

assessment are advised to consider oversight gaps, incentives and targets, staff churn, use of new technology, sector indicators and territorial issues, and plan for emergencies.

The key message is that fraud risks are not uniform. A retailer with complex supply chains faces different challenges to a tax consultancy advising multinational groups. Regular risk mapping helps identify specific vulnerabilities.

3.3 Proportionate, risk-based procedures: Controls should reflect the organisation's risks, size and the degree of control over the actor: typically tighter controls for employees, and contractual and oversight measures for third parties acting on the organisation's behalf. The Guidance warns against treating existing audit and regulatory controls as a safe harbour; they should be analysed against identified risks. Decisions not to adopt a measure should be documented.

Again, the measures will be context sensitive, for instance, for a professional services firm, this may mean stricter client onboarding and review of billing practices; for a construction company, tighter oversight of subcontractor claims.

3.4 Due diligence: The Guidance emphasises the importance of proportionate checks on those who perform, or will perform, services for or on behalf of the organisation, and to key transactions. Third parties often present the greatest risk. Appropriate measures include screening and verification where appropriate, suitable contractual terms (including termination rights for fraud), periodic refresh, attention to pressure indicators in higher-risk roles, and M&A diligence that covers criminal/regulatory history, tax position and the maturity of the target's fraud controls.

3.5 Communication (including training): Firms are advised to ensure policies and procedures are communicated and understood across the organisation and by relevant third parties, with training on the new offence. In many cases it will be appropriate to maintain whistleblowing arrangements, and, where suitable, the publication of the outcomes of investigations.

Policies are only as good as employees' awareness of them. Interactive training, practical case studies, and confidential whistleblowing channels can all reinforce the culture of prevention.

3.6 Monitoring and review: Fraud risks evolve quickly, particularly with advances in technology and AI-enabled crime. As such, the guidance encourages firms to implement measures to detect and investigate fraud and to monitor the control environment on an ongoing basis. Particular measures advised include analysis of procurement, payment and invoicing data, access monitoring, a named individual reporting fraud risk management to the board, investigations that are independent and fairly conducted, and tracking of fraud control performance. The Guidance emphasises the importance of learning from incidents and sector developments.

What this means in practice

The key imperative is reasonableness. The guidance does not prescribe a checklist; instead, it expects organisations to make proportionate decisions, document them, and revisit them as circumstances change.

Consider two examples:

- A financial services firm might identify the risk of employees manipulating client portfolios to generate higher fees. Reasonable procedures could include automated monitoring of transaction patterns, coupled with clear escalation routes for anomalies.
- A manufacturing business may face exposure through false invoicing by suppliers. Reasonable steps could involve segregation of duties in accounts payable, periodic supplier audits, and whistleblower incentives.

In both scenarios, it is not perfection that is required, but evidence that the company took active, proportionate and evolving measures to mitigate its specific risks.

Enforcement outlook

Both the Serious Fraud Office and the Crown Prosecution Service have been vocal in welcoming the new offence. They have warned that enforcement is not a distant prospect: companies should expect investigations to begin in short order.

The potential consequences are stark. Conviction could bring unlimited fines, exclusion from public contracts and reputational harm. On the other hand, in England and Wales, organisations that self-report and cooperate may be able to resolve matters through a Deferred Prosecution Agreement (DPA).

Conclusion

The failure to prevent fraud offence marks a decisive shift in corporate criminal liability. Large organisations must now take ownership of fraud prevention in the same way they have with bribery and money laundering.

For boards and compliance teams, the immediate priorities are to:

- conduct or strengthen fraud-specific risk assessments;
- identify and address gaps in existing controls;
- embed fraud awareness into training and culture; and
- ensure top-level oversight.

This is more than a legal requirement; it is a business imperative. Companies that treat compliance as a box-ticking exercise risk exposure. Those that invest in a genuine anti-fraud culture will not only protect themselves against liability and financial loss but also build trust with clients, regulators and the public.

- Nick Scott, Partner, Keystone Law. Christopher Coltart KC, Christopher Veal and Richard Edmond, 2 Hare Court chambers