Fraud prevention or financial fallout? Navigating the new failure to prevent fraud offence

Paul Henty, Partner, and Deen Taj, Solicitor, with Beale & Co Solicitors LLP explore the new offence of failure to prevent fraud created by the UK Economic Crime and Corporate Transparency Act 2023

The Economic Crime and Corporate Transparency Act 2023 (the "Act") represents a landmark piece of legislation in the UK's fight against corporate fraud and other economic crime. The Act received Royal Assent on 6 December 2023. However, many of its provisions were not scheduled to come into effect until a later date.

One such provision is arguably the most important. The "failure to prevent fraud" offence (the "Offence") (s.199 of the Act) aims to address persistent accountability gaps within organisations and ensure that they take proactive steps to deter fraudulent activity.

The Offence, which will come into effect on 1 September 2025, has implications for a wide range of entities operating within the UK and beyond. It significantly reduces the scope for businesses to escape liability for fraudulent acts committed by employers or subsidiaries, particularly where the organisation could have received a direct or indirect benefit from the fraudulent conduct.

"So what?", you may ask. "Haven't companies been prosecuted under the fraud statutes before?". Yes, they have. However, in order for prosecutors to secure a conviction they must tie the relevant conduct to an individual whose conduct and state of mind can be attributed to the company, so that he/she represents the company's "directing mind and will". For example, Bob may be at fault for issuing a false invoice to his employer's customer, but this is Bob's problem and not necessarily the company's, particularly if nobody else at the company had any idea what Bob was up to.

The new offence creates a stricter, secondary or vicarious liability where the relevant company is considered at fault for not doing enough to prevent the wrongdoing by employees or subsidiaries in the first place, regardless of whether it knew about it or not.

The Home Office recently published guidance to organisations on the offence of failure to prevent fraud (the "Guidance"). Some of this is discussed below. This is a particularly important guide for understanding a complex and important criminal offence, the commission of which could do untold harm to an organisation's hard-won reputation, not to mention the risk of penalties against its directors.

Below we explore the Guidance and the implications for organisations within its remit.

An overview of the Act

The Act is part of a broader strategy to address economic crime, including fraud, corruption, and money laundering, which reportedly costs the UK economy £219 billion annually (Annual Fraud Indicator 2023 by Peters & Peters and Crowe). It builds on earlier initiatives, such as the Bribery Act 2010 and the Criminal Finances Act 2017, expanding the scope of corporate liability while introducing new compliance obligations.

Key provisions of the Act include reforms to Companies House aimed at improving the accuracy and reliability of corporate data, as well as enhanced checks on company directors and beneficial owners. The Act also strengthens powers for law enforcement to seize and recover illicit assets and introduces new mechanisms to disrupt the use of opaque corporate structures for criminal purposes. These measures are complemented by the new Offence which is aimed at ensuring that organisations take active steps to deter fraud committed by employees, agents, or other associated persons. Together, these provisions reflect an increasing emphasis on corporate accountability and proactive risk management.

Key features of the Offence

The Offence applies to relevant bodies, including companies, partnerships, and other legal entities. However, liability is limited to "large organisations" that meet at least two of the following criteria:

- turnover exceeding £36 million;

- balance sheet total exceeding £18 million;
- more than 250 employees.

Firms in scope include businesses across all sectors that meet these thresholds, from financial institutions to manufacturing, technology, and professional services companies.

Small and medium-sized enterprises (SMEs) are exempt from the Offence, reflecting the government's attempt to balance compliance burdens with proportionality. However, SMEs may still face indirect exposure through partnerships with larger organisations. This is likely to take the form of contractual anti-fraud compliance obligations and requirements to submit to due diligence measures.

"Key provisions of the Act include reforms to Companies House aimed at improving the accuracy and reliability of corporate data, as well as enhanced checks on company directors and beneficial owners. The Act also strengthens powers for law enforcement to seize and recover illicit assets and introduces new mechanisms to disrupt the use of opaque corporate structures for criminal purposes"

Pursuant to s.199, an offence is committed when an associated person, such as an employee, agent, or contractor, commits a base fraud offence, with the intention to benefit the organisation, whether directly or indirectly. Effectively, s.199 provides that the organisation is vicariously liable for certain acts of its associated persons or entities where they commit one of the base offences.

What are the base offences?

To re-cap, in order for s.199 to be engaged, an associated person of an in-scope organisation must commit a base offence. These are listed in Schedule 13 to the Act.

For England and Wales, the range of base fraud offences includes the following:

- Fraud by False Representation (Section 2, Fraud Act 2006): Example: A company director submits falsified financial statements to secure a business loan, falsely claiming the company is profitable when it is not.
- Fraud by Failing to Disclose Information (Section 3, Fraud Act 2006): Example: An employee fails to disclose a conflict of interest when awarding a contract, knowing that their spouse owns the vendor company, thereby gaining an unfair advantage.
- Fraud by Abuse of Position (Section 4, Fraud Act 2006): Example: A finance manager uses their position to divert company funds into their personal account, abusing the trust placed in them.
- Participation in a Fraudulent Business (Section 9, Fraud Act 2006): Example: A director continues trading while knowing the company is insolvent, taking customer payments for goods they cannot deliver.
- Obtaining Services Dishonestly (Section 11, Fraud Act 2006): Example: An employee uses a stolen credit card to book a company conference venue, avoiding payment themselves.
- Cheating the Public Revenue (Common Law): Example: A company underreports its taxable income by fabricating expense claims, thereby evading substantial tax payments.
- False Accounting (Section 17, Theft Act 1968): Example: An accountant manipulates company ledgers to show non-existent revenue, inflating profits to attract investors.
- False Statements by Company Directors (Section 19, Theft Act 1968): Example: A director signs off on a prospectus with knowingly inflated revenue figures to mislead potential investors.
- Fraudulent Trading (Section 993, Companies Act 2006): Example: A director operates a Ponzi scheme under the guise of a legitimate investment firm, taking investor funds to pay off earlier investors.

For Scotland, the list of base offences omits the Fraud Act 2006 but includes the common law offences of fraud, uttering, and embezzlement. In contrast, the Northern Ireland list includes the same references to the Fraud Act 2006 as for England and Wales, the offence of cheating the revenue and ss 17 and 19 of the Theft Act Northern Ireland 1969.

In order for s.199 to be activated, the relevant act or omission must have been intended to benefit the organisation (directly or indirectly). However, that does not need to be the only objective. Individuals may, for example, make fraudulent statements to win new work in order to meet their bonus targets rather than to further the ends of the organisation. The fact that this will also help the organisation by winning a new account is sufficient to trigger s.199. That is the case regardless of whether or not the senior personnel of the company knew about the misrepresentations.

One limitation, though, is that the organisation will have a defence where it is itself the victim of the fraud. If, for example, the relevant fraud entails the employee making artificial expenses claims (e.g. a business trip that was really a private holiday), the organisation will have a defence in any related prosecution.

(Continued on page 4)

(Continued from page 3)

Defences

Where charged with committing the Offence, there are two available defences, the first being that the organisation was itself a victim of the fraud. The second and more important defence is that the organisation had in place such prevention procedures as it was reasonable in all the circumstances to expect the body to implement (s.199(4)). In this regard, "procedures" means those systems which are designed to prevent persons associated with the body from committing fraud offences.

The government's Guidance, published alongside the Act, provides detailed direction on designing and implementing these procedures. Organisations are expected to conduct regular and thorough evaluations of fraud risks specific to their activities, geographic presence, and sectoral vulnerabilities. For instance, firms operating in high-risk jurisdictions or industries prone to corruption must allocate resources proportionate to these risks. Senior management must demonstrate a culture of integrity and accountability, embedding anti-fraud measures into the organisation's ethos.

Prevention measures should be tailored to the organisation's size, nature, and complexity. These may range from automated transaction monitoring systems for large multinational firms to simpler manual checks for smaller entities. Robust vetting processes for employees, contractors, and business partners are essential, as are regular communications and tailored training sessions to raise awareness of anti-fraud policies. Mechanisms to monitor and review the effectiveness of these measures, including internal audits, data analytics, and whistleblowing hotlines, are also critical.

The Offence's extraterritorial reach ensures that fraudulent conduct both within and outside the UK may be captured, provided that there is a UK nexus, for example that one of the acts which was part of the fraud took place in the UK, or the gain or loss from the fraudulent conduct occurs in the UK. Convicted organisations may face unlimited fines, reputational damage that could affect shareholder confidence and customer trust, and increased scrutiny from regulators, investors, and the public. The organisation could also be excluded from public contract opportunities under s.57 of the Procurement Act 2023.

To many this defence will be familiar. Under s.7(1) of the Bribery Act 2010, the offence of "failure to prevent bribery" by associated persons was created. Similarly, s.7(2) provided a defence for organisations who could show that they "had in place adequate procedures designed to prevent persons associated with [it] from undertaking such conduct". This sparked nearly all organisations of a certain size to introduce relevant policies and bribery training. It can be expected that organisations will do likewise to avoid the risk of committing the Offence.

"Prevention measures should be tailored to the organisation's size, nature, and complexity. These may range from automated transaction monitoring systems for large multinational firms to simpler manual checks for smaller entities. Robust vetting... processes are essential, as are regular communications and tailored training sessions to raise awareness of anti-fraud policies"

However, in our view, preventing fraud is substantially harder than preventing bribery. As the list of base offences shows, the breaches can be committed in a wider range of situations. Bribery is also often committed by one or both parties knowingly engaging in "improper performance" of their work role. This is not always required for fraud to be committed.

A person, for example, who makes exaggerated claims about their employer's experience so their company can win a tender, may be wholeheartedly acting to benefit their company rather than themselves. Bribery is also only engaged in situations where there is an interaction between two or more parties. Fraud can be committed in a wider range of contexts.

The Guidance: key insights

The Guidance provides a comprehensive framework for organisations to implement effective fraud prevention measures. It highlights the importance of a proactive and tailored approach to compliance, urging organisations to focus on the specific risks they face.

Risk assessment

A cornerstone of the Guidance is the need for regular and detailed fraud risk assessments. These assessments should consider the organisation's size, sector, operational geography, and relationships with third parties. For example, firms operating in high-risk jurisdictions or industries prone to bribery and corruption must allocate resources proportionate to these risks.

Leadership and culture

The Guidance also emphasises the critical role of senior leadership in fostering a culture of compliance. Leadership must visibly support fraud prevention efforts and communicate the organisation's commitment to ethical practices. Anti-fraud measures must be embedded into corporate governance structures to ensure alignment across all levels of the organisation.

Proportionality in procedures

The Guidance highlights that fraud prevention measures must be proportionate to the organisation's size, structure, and risk profile. Smaller firms might focus on manual oversight mechanisms, while larger firms are encouraged to deploy sophisticated technologies such as transaction monitoring systems or artificial intelligence tools. The procedures should evolve as the organisation grows or encounters changes in its risk landscape.

Due diligence

Robust due diligence processes are another focal point of the Guidance. This includes verifying the integrity of employees, contractors, and business partners to ensure that they align with the organisation's ethical standards. Enhanced due diligence may be necessary for high-risk roles or partnerships, such as those involving financial transactions or procurement.

Whistleblowing mechanisms

Organisations must establish whistleblowing systems that are accessible, well-publicised, and supported by strong confidentiality protections. The Guidance encourages organisations to promote a culture where employees and third parties feel safe reporting suspicious activities.

Fraud indicators and red flags

The Guidance advises organisations to remain vigilant to common fraud indicators, such as unusual transaction patterns, sudden changes in employee behaviour, or discrepancies in documentation. Organisations should train staff to identify and act upon these red flags.

Monitoring and review

Organisations must establish robust monitoring and review mechanisms to ensure their fraud prevention measures remain effective. This includes periodic audits, the use of data analytics to identify anomalies, and whistleblowing hotlines to encourage the reporting of suspicious activities. Continuous review and adaptation are critical to addressing emerging risks.

Incident response plans

The Guidance recommends having a robust response plan for suspected fraud incidents. This plan should include immediate containment measures, internal investigations, and regulatory notifications where appropriate.

Alignment with broader compliance obligations

The Guidance encourages organisations to integrate fraud prevention measures with other regulatory frameworks, such as anti-money laundering protocols, data protection regulations, and anti-bribery policies. This holistic approach not only strengthens the organisation's overall compliance posture but also reduces redundancies and enhances efficiency.

Supply chain integrity

Organisations are advised to conduct due diligence not only on direct business partners but also on their suppliers and subcontractors. This is particularly important for industries with complex supply chains, where risks may be hidden deeper within the network.

Documentation and evidence

The Guidance places significant emphasis on the need for meticulous documentation. Organisations must be able to demonstrate the implementation and effectiveness of their prevention measures, particularly in the event of an investigation or prosecution. Comprehensive records of risk assessments, training sessions, and monitoring activities serve as valuable evidence of compliance.

S.199 and the connection with ESG statements

Many commentators have pointed to the risk that s.199 creates where organisations make ESG related claims about their products. The risk could also attach when making mandatory disclosures under legislation such as s.54 of the Modern Slavery Act 2015. S.54 requires companies with an annual turnover above £36 million to disclose the steps they take (if any) to ensure that there is no slavery or human trafficking present in their organisation or supply chain.

Often, environmental claims about products will be positioned on packaging merely to attract customers or reassure them that they are making ethical purchase choices. For services, it is possible for similar declarations to be made on websites or promotional literature.

In order to enhance the credentials of the organisation, its employees or directors may be tempted to exaggerate its ESG profile (or withhold less flattering information about the organisation), so as not to alienate existing customers or to win new ones. There is an elevated risk from doing this, given that these actions could constitute fraud by representation (s.2 Fraud Act 2006) or fraud by failing to disclose information (s.3 Fraud Act 2006).

Recent enforcement action by the UK Competition and Markets Authority (CMA) in relation to its Green Claims code highlights both the risk of detection as well as providing useful examples of how environmental claims can stray into being misleading.

In 2024, for example, the CMA investigated the UK fashion industry and producers of FMC goods. These were ultimately settled with undertakings in all if not most cases. However, they provide some useful information about how businesses can go wrong. Problematic claims included the use of vague and broad eco-statements, for example packaging or marketing a product as 'sustainable' or 'better' for the environment without relevant evidence; misleading claims about the use of recycled or natural materials in a product and how recyclable

it is; and entire ranges being incorrectly branded as 'sustainable'.

It is possible that in future cases a criminal prosecutor could bring charges against an organisation on the basis of information uncovered by the CMA's investigations.

Extraterritoriality: is it good for the UK?

Another striking feature of the Offence is that it will apply to overseas organisations who do business in the UK. For example, a Canadian multinational could find itself liable for fraud committed by its UK subsidiary. That may be the case even where the UK business runs autonomously with little input from its parent.

Whilst this will undoubtedly make life easier for prosecutors in cross-border situations, some have questioned whether it is good for the UK economy. The UK Law Society, for example, flagged in the consultation process that this aspect of the new law may render the UK less attractive as an investment destination for overseas-based multinationals fearing repercussions from any wayward conduct by their UK colleagues.

Implications and next steps for organisations

The introduction of the Offence necessitates a comprehensive reassessment of fraud risk management frameworks by affected organisations. For large businesses, the burden of compliance requires immediate and sustained attention. Organisations must establish or enhance procedures to align with the six principles outlined in the Guidance.

One of the most pressing implications is the need to allocate resources effectively. Firms must ensure that they dedicate adequate funding and personnel to fraud prevention initiatives. This may involve the deployment of advanced fraud detection technologies, such as artificial intelligence-driven data analysis tools, to identify and mitigate risks more efficiently.

Cross-departmental collaboration is another critical requirement. Legal, compliance, finance, and human resources teams must work together to embed anti-fraud measures into the organisation's operational and governance structures. Training programmes, while essential, must be integrated into broader efforts to cultivate a culture of integrity across all levels of the organisation.

Board engagement is indispensable in ensuring the effectiveness of fraud prevention measures. Boards should regularly review fraud risk assessments, approve policies and procedures, and receive updates on the organisation's compliance efforts. Active board oversight helps to reinforce the importance of fraud prevention as a strategic priority and ensures accountability at the highest level.

For legal practitioners, the Offence presents opportunities to guide clients through complex compliance landscapes. Practitioners can play a pivotal role in conducting gap analyses to identify deficiencies in existing procedures and providing tailored recommendations to address these gaps. Advising on the integration of fraud prevention measures with other regulatory obligations, such as GDPR and AML requirements, can further enhance organisational resilience.

Failure to prepare adequately for the Offence's requirements poses significant risks. Beyond the financial penalties associated with non-compliance, organisations face reputational harm that could deter investors, erode customer trust, and attract heightened regulatory scrutiny. A damaged reputation is often harder to repair than financial loss and can have long-lasting consequences for the organisation's competitive position.

For multinational organisations, the extraterritorial reach of the Offence requires a coordinated, cross-jurisdictional approach to compliance. Organisations must ensure that fraud prevention measures align with the varying legal requirements in different countries while maintaining a consistent ethical framework across all operations. This adds a layer of complexity that requires robust management and careful planning.

Ultimately, the Offence is a catalyst for organisations to prioritise ethical business practices, enhance governance structures, and foster a culture of accountability. The September 2025 implementation date provides a crucial window for preparation. Organisations that act proactively can position themselves as leaders in corporate integrity, mitigating both legal risks and reputational damage. By embracing the principles set out in the Guidance and taking concrete steps to prevent fraud, businesses can play a pivotal role in combating economic crime and promoting trust within the markets in which they operate.

Whilst the introduction of this Offence may seem daunting, it also presents an opportunity for organisations to strengthen their governance frameworks and lead with integrity. By taking proactive steps now, businesses can not only mitigate risks, but also enhance trust with stakeholders and contribute to a fairer marketplace. With that said, are you ready for September?

Paul Henty

Deen Taj

Beale & Co Solicitors LLP

p.henty@beale-law.com

d.taj@beale-law.com