The UK economic crime & corporate transparency act 2023

What companies need to know and what they can do to prepare

Speed read

- *The UK Economic Crime & Corporate Transparency Act 2023* sets out two major reforms making it much easier for UK authorities to prosecute corporate wrongdoing:

  (1) it substantially increases the circumstances in which a company can be held liable for crimes committed by their employees. Now, relevant offences committed by a company's **'senior managers'** can be attributed to the company.

  - This reform came into force on 26 December 2023; and

  (2) it introduces a new corporate offence of **'failure to prevent fraud'**, which criminalises companies that fail to prevent persons associated with them from committing a range of fraud offences. A company has a full defence where it had in place 'reasonable procedures' to prevent the fraud from occurring.

  - On 6 November 2024, the UK government published its long-awaited guidance as to the new offence and the meaning of 'reasonable procedures'; at the same time, it announced that the offence will come into force on 1 September 2025.

- These reforms constitute the most significant change to corporate criminal liability in the UK for decades. In addition, both of these provisions have **extra-territorial effect**, meaning that the actions of individuals and companies located abroad can be prosecuted in the UK as long as there is a sufficient link to the UK.
- This article summarises these key aspects of the new legislation and (i) sets out what companies can do now in order to mitigate risks already posed by the 'senior manager' reform; and (ii) outlines what companies should be doing to prepare for the new 'failure to prevent' offence coming into force.

(1) Introduction

Provisions contained within the UK *Economic Crime & Corporate Transparency Act* 2023 (**"ECCTA"**) represents the most fundamental change in living memory to the financial crime and compliance framework in the UK. Due to its broad scope and wide extra-territorial reach, ECCTA will have a seismic effect on the risk landscape faced by multinational companies with links to the UK.

In the past, establishing corporate criminal liability (especially on the part of non-UK companies) was very difficult due to the 'Identification Principle' in English law. In effect, a prosecutor had to prove that the board (or people with specific authority delegated to them by the board) were involved in the relevant crime in order for their conduct to be imputed to the company. Legislation in both 2010 and 2017 sought to modify that position in relation to the specific offences of bribery and the facilitation of tax evasion. However, ECCTA significantly broadens criminal liability for companies in relation to a wide range of economic crimes, with the result that the UK regime is now much closer to that of the USA.

The process of circumventing the Identification Principle began with the implementation of the UK Bribery Act 2010 (**"UKBA"**), which introduced a corporate offence of failing to prevent bribery, and the UK *Criminal Finances Act* 2017 (**"CFA"**), which introduced a corporate offence of failing to prevent the facilitation of tax evasion. In both cases, the laws have wide extra-territorial effect.

However, **ECCTA goes significantly beyond this** by introducing (amongst other things):

(1) liability on the part of companies for the criminal acts of their **"senior managers"** in relation to a wide range of economic crimes. Previously, companies could only be liable for the criminal acts of their board members or others with specific authority delegated to them. This change in the law significantly widens the set of individuals that can expose a company to criminal liability. Crucially, and unlike the 'failure to prevent' offences under the UKBA and the CFA, it is no defence for the company to show that it had appropriate procedures in place that were designed to prevent the wrongdoing.

- This **"Senior Manager Regime"** came into force on 26 December 2023; and

(2) a new corporate offence of **failing to prevent fraud** (the **"FTP Fraud Offence"**). This is similar in design to the 'failing to prevent' offences referred to above. However, given the broader scope and more widespread nature of fraud, the new law will cover a much wider range of conduct. Under the new FTP Fraud Offence, criminal liability can effectively attach to large companies on a **strict liability** basis for the frauds committed by their employees, service providers and other 'associated persons' (even if senior management was unaware of the conduct). The only defence to the FTP Fraud Offence is for the company to show that it had 'reasonable prevention procedures' in place to prevent the fraud.

- On 6 November 2024, the UK government published official guidance as to the meaning of 'reasonable prevention procedures'. At the same time, it announced that the FTP Fraud Offence will come into force on 1 September 2025.

It is important to note that these reforms can also apply to the conduct of individuals and companies based outside of the UK.

(2) The senior manager regime

Until recently, the main way in which a company could be held criminally liable under English law for the acts of its employees was where the employee was acting as the **directing mind and will ("DMW")** of the company. In general, only the board or those to whom the board had explicitly delegated authority would be capable of constituting a company's DMW. This led to difficulties in prosecuting companies, as evidence implicating such individuals was generally hard to find, or it was often more junior employees who engaged in the relevant conduct.

However, since 26 December 2023, it has been possible for companies to be held criminally liable for relevant offences committed by their "senior managers", where they are acting within the actual or apparent scope of their authority. This power is additional to powers that UK prosecutors already have to prosecute individuals for the same offence.

For these purposes:

– "**relevant offences**" include a wide range of criminal offences that are relevant to companies, including fraud, bribery, theft, false accounting, money laundering, financial regulatory and tax-related offences (Schedule 12 ECCTA contains the full list of relevant offences)[1]; and

[1] Under the previous Conservative government, a Criminal Justice Bill proposed expansion of the law to include any criminal offence (rather than just those listed in Schedule 12 ECCTA). It is possible that this proposal will be revived under the new Labour government.

– "**senior managers**" are individuals who play a **significant role** in:

  - the making of decisions about how the whole, or a substantial part, of the activities of the company are to be managed or organised; or
  - the actual managing or organising of the whole, or a substantial part, of the company's activities.

  Importantly, guidance states that senior individuals within non-executive, non-client facing roles (such as Legal, Finance, Human Resources or Compliance departments) can satisfy the definition of being a senior manager. The test is one of fact in accordance with the definition in the statute; it is, therefore, irrelevant what is stated on a person's business card or contract of employment.

Under section 196 of ECCTA, a company (wherever incorporated) can be liable for the criminal acts of their senior managers wherever they take place, subject to the jurisdictional reach of the underlying criminal offence.[2]

It is important to note that the Senior Manager Regime is distinct from the Senior Manager & Certification Regime ("**SMCR**") administered by the UK Financial Conduct Authority. While there may be an overlap in an organisation between those who are senior managers under ECCTA and senior managers under the SMCR, the underlying legal tests and resultant responsibilities are different and should be considered separately.

The Senior Manager Regime could lead to criminal liability for a non-UK company in a great number of scenarios. Examples may include where:

– board members of a US company approve the contents of an annual report which falsely misrepresents environmental data to potential investors in the UK;

– the Head of Compliance in a French company signs off on an insurance claim underwritten in the UK, knowing that it is exaggerated;

– a Head of Sales of a Japanese company with operations in the UK via a branch or subsidiary makes false representations about its products to a customer;

– a Head of Finance in an Italian company instructs a team member to send back-dated invoices to a UK auditor in order to inflate revenues for a particular financial period;

– the Head of Corporate of a UAE company who is a UK national signs a deal with a company that she suspects is owned by a sanctioned Iranian businessman3;

– a Senior Account Manager employed by a US company instructs their team to inflate invoices to be sent to a UK-headquartered client.

The conduct of just one senior manager is sufficient for the company to commit the relevant offence – it can be held liable even if no other directors or senior managers were aware of, or involved in, the conduct.

Importantly, a company can be criminally liable under this legislation **even where it has implemented reasonable prevention procedures.** However, such procedures are of course vital in reducing the risk of the wrongdoing occurring in the first place (and may be a factor in favour of the courts imposing a lower sentence in the event of a conviction under section 196 of ECCTA).

[2] The jurisdictional tests are not the same for each relevant offence. For example, the jurisdictional test for bribery differs from that for fraud. When applying the jurisdictional test for the specific relevant offence to a company, it is to be assumed that the company engaged in the relevant acts instead of the senior manager.
[3] Note that UK sanctions laws apply to all UK nationals, wherever they are situated in the world.

(3) the failure to prevent fraud offence

The FTP Fraud Offence comes into force on 1 September 2025. In short, it is a crime where a company fails to prevent fraud. The provisions of the legislation only apply to "**large organisations**", meaning those meeting two of the following three criteria **across their whole group**:

– over 250 employees;

– over £18 million in total assets; and/or

– over £36 million turnover.

Under section 199 of ECCTA, a large organisation ("**O**") will commit an offence where an "associate" of O commits a fraud offence intending to benefit O or someone to whom the associate provides services on behalf of O.

Importantly, a large organisation can commit the FTP Fraud Offence even if incorporated outside of the UK. All that is required is that there is a relevant UK link to the fraud (such as UK victims, UK conspirators or where part of the relevant conduct took place in the UK). As a result, by way of example, a Japanese company could be criminally liable in the UK for failing to prevent an employee or service provider in Germany from engaging in a fraud that has an impact in the UK.

For these purposes:

– "**associate**" means an employee, agent or subsidiary of the organisation, or **someone who otherwise performs services for or on behalf of** the organisation. This is extremely broad, and can cover the full range of third parties that provide services for or on behalf of a company; and

– "**fraud**" includes fraud offences under the UK *Fraud Act* 2006, false accounting under the UK *Theft Act* 1968 and the common law offence of cheating the public revenue (Schedule 13 of ECCTA contains the full list of fraud offences).

Accordingly, large companies can commit the FTP Fraud Offence even if none of their management are aware of, or involved in, the fraud. However, a company cannot be guilty of an offence if it was the victim of the fraud.

Examples of when the new FTP Fraud Offence may be committed by a company include:

– an employee (or service provider) of a US company makes false representations about its products to a UK customer;

– an employee (or service provider) of a Japanese company (when based in the UK via a branch) makes false representations about its products to a customer (wherever located);

– an employee (or service provider) of a Mexican company makes a false statement to the UK tax authority so as to reduce or avoid the payment of tax;

– an employee (or service provider) of a Canadian company misdescribes a commission as a consultancy fee in order to hide the fact of the commission from a third party based in the UK;

– the directors of a Japanese company approve false or misleading statements in a prospectus to investors on the London Stock Exchange; and

– the directors of a UK company approve false or misleading statements in a prospectus to investors outside the UK.

Upon conviction, the courts can impose unlimited fines that will be calculated in accordance with the relevant sentencing guidelines.

It is important to note that a full defence exists where a company has implemented "**reasonable prevention procedures**". Guidance as to the meaning of "reasonable prevention procedures" was published by the UK government on 6 November 2024 and the offence itself will be in force from 1 September 2025.

There are steps that can be taken immediately to ensure that companies are properly prepared for the FTP Fraud Offence. Companies should note that undertaking associated risk assessments, and designing and implementing appropriate procedures, are likely to take some time, if done properly, and that obtaining access to expert advice is likely to be more difficult the closer it gets to September 2025.

(4) What should companies do now?

There is no 'one size fits all' approach for companies to adopt. The measures required to protect a company are dependent on the specific risks faced by the company, including where, how and with whom it does business. Certain risks are known to exist in certain industries and certain countries, or when dealing with third parties and joint venture partners in unfamiliar markets.

In relation to the Senior Manager Regime, a simple - but effective - 'first step' in the short term would be to ensure that the senior managers across an organisation are identified and, along with their deputies and key team members, provided with enhanced compliance training. This training should reinforce what behaviours are unacceptable and underscore the importance of complying with applicable laws and company policies.

As regards the FTP Fraud Offence, a first step would be to consider the UK government guidance as to the meaning and scope of 'reasonable prevention procedures' under ECCTA. While this guidance is not binding in law, it is highly likely that prosecutors and courts would consider it when assessing the reasonableness of a company's fraud prevention policies and procedures.

As with the previous corporate criminal offences under the UKBA and the CFA, the UK government's guidance published under ECCTA is underpinned by six key principles that should inform the approach taken by companies to their fraud prevention programmes. These are as follows:

- **risk assessments**: companies should assess the nature and extent of the risks of fraud by their associated persons. This requirement is vital as it will help to determine what proportionate policies and procedures will look like in the specific circumstances of a company and those areas where it should focus its attention. To that end, the guidance states that "*it will rarely be considered reasonable not to have even conducted a risk assessment*" and that risk assessments should be dynamic, documented and reviewed regularly;
- **proportionate risk-based prevention procedures**: policies and procedures should be proportionate to the risks faced by a company and to the nature and complexity of company's activities. This means that more robust measures will be required where the risks are higher;
- **top level (board) commitment**: the senior management of a company must communicate its commitment to rejecting fraud throughout the company and fostering a culture of compliance. 'Senior management' is not defined in any detail for this specific purpose, but the guidance published under ECCTA suggests that senior managers under the SMCR may be an appropriate benchmark for regulated firms to use;
- **communication and training**: it is not enough for a company to put into place new policies, they have to be implemented and form part of the fabric of how a company does business. An

important aspect of that is ensuring that personnel are trained as to fraud risks and the nature of the company's policies and procedures (including those relating to whistle-blowing);

– **due diligence**: companies should undertake proportionate and risk-based due diligence into those persons who perform services for or on their behalf; and

– **monitoring and review**: policies and procedures relating to fraud detection and prevention must be monitored regularly to ensure that they are fit for purpose and effective. Where areas for improvement are identified, the company should take steps to implement them.

Given the above guiding principles, we strongly advise that companies should arrange for senior managers and their key team members to receive appropriate training as to risks relating to fraud and other economic crime and the best practices in mitigating them. This should be done urgently as it would provide an additional layer of protection while a robust risk assessment can take place. Regulated firms may wish to ensure that those designated as senior managers under the SMCR are included within the pool of employees subjected to this training (even if they might not strictly fall under the senior manager definition under ECCTA). Such training would ideally be refreshed periodically and re-run for new joiners or those who missed it.

As for the FTP Fraud Offence, one of the most important first steps would be to undertake a detailed fraud risk assessment in order to determine the areas of highest risk across the business The methodology for conducting a safe and reliable risk assessment is crucial. Certain tasks should be undertaken by certain persons, in a particular way and in a particular order. Data and documents need to be gathered, analysed and recorded according to a carefully devised protocol.

After a dedicated fraud risk assessment, it will be necessary for companies to design and implement proportionate policies and procedures to help ensure that the 'reasonable prevention procedures' defence to the FTP Fraud Offence will be available to them. We expect that auditors will seek confirmation as part of annual audits that companies they have taken these steps. Similar questions are also being asked as part of the due diligence process for corporate acquisitions and by other interested stakeholders such as insurers, bankers and investors.

(5) Methodology of risk assessments is key

When drafting a written risk assessment, it is important to avoid inadvertently creating a disclosable 'road map' to key risks, persons and issues in the organisation, or recording issues or making recommendations in a way that unnecessarily highlights issues or weaknesses in the past. What is contained in the risk assessment, and how matters are described, is therefore very important. The risk assessment should be undertaken by experienced lawyers who can gather required information in a privileged context. Fraud risk assessments should also be updated periodically.

Whether or not legal privilege applies or is asserted, it should be assumed that various regulators and other stakeholders may try to obtain access to the risk assessment document – or at least to key findings and recommendations. Alternatively, the company may choose to waive privilege. As a result, the risk assessment (and related work product) must be carefully compiled and drafted. Language must be precise and assessments must be balanced, credible and supportable. Be prepared to manage those with an interest in seeking access to the risk assessment (such as auditors, bankers, insurers, investors, regulators, suitors in M&A transactions and possibly opponents in litigation).

It is also important to remember that parties in the UK 'regulated sector' for the purposes of the UK Proceeds of Crime Act 2002 (e.g., auditors, bankers, third party lawyers, etc.) have a duty to report suspected money laundering to the UK National Crime Agency by way of a suspicious activity report. Failure to do so is a criminal offence.

If issues of particular sensitivity are discovered during the risk assessment process, it may be desirable to 'quarantine' them into a separate advisory environment or investigation, so that the issues can be protected by legal privilege and do not taint the risk assessment process. A key objective is to resolve such issues before the process is completed and conclusions are stated in the risk assessment document.

The UK government guidance on ECCTA states that investigations should be "independent, appropriately resourced and scoped (including through legal advice) and legally compliant" and that "**useful sources of information include the 'Global Practitioners Guide to Investigations**'". Our team at McDermott Will & Schulte drafted the two most pertinent chapters in that Guide for the past three years.4

All of the above considerations impact timing, process and cost. To avoid common pitfalls and ensure that resources are appropriately targeted, companies should give consideration to the methodology for such a sensitive project before work commences.

(6) Conclusion

At a time of widespread global conflict and economic stress, and against a background in which more than 70 countries held national elections in 2024, significant change is inevitable. Economic and political turmoil is likely to give rise to more fraud, anti-competitive behaviour, non-compliant business practices, increased credit default events and insolvencies.

ECCTA provides UK law enforcement agencies with tools they never had before and the ability to prosecute companies in circumstances where it was not previously possible. By preparing proactively for the impact of ECCTA, multinationals can better insulate themselves for the potential uncertainties to come and can even secure competitive advantage by using strong compliance as a differentiator.

McDermott's Investigations & Compliance team has decades of experience helping multinational organisations navigate the UK's increasingly challenging compliance environment, has advised on the design and implementation of compliance procedures, and has acted on some of the highest profile corporate investigations and resolutions in recent years.

Please contact us if you wish to discuss any of the issues in this note.

Key contacts

Simon Airey
Partner, Global Co-Head of Investigations & Compliance

sairey@mwe.com
+44 77 3802 3802

James Dobias
Counsel

jdobias@mwe.com
+44 20 7575 0319

Andrew Butel
Counsel

abutel@mwe.com
+44 20 7575 0323

William Merry
Senior Associate

wmerry@mwe.com
+44 20 7577 6910

[4] https://globalinvestigationsreview.com/guide/the-practitioners-guide-global-investigations/2025/article/beginning-internal-investigation-the-uk-perspective https://globalinvestigationsreview.com/guide/the-practitioners-guide-global-investigations/2025/article/united-kingdom-overview-of-the-corporate-criminal-liability-regime-and-recent-major-developments