fieldfisher

Guide to the Economic Crime and Corporate Transparency Act 2023

April 2024

Contents

Overview

The Economic Crime and Corporate Transparency Act 2023 ("**ECCTA**") received Royal Assent on 26th October 2023. Widely recognised as the most significant overhaul of corporate criminal liability since the introduction of the Bribery Act 2010, ECCTA[1] has three key aims:

(a) to improve transparency over UK companies;

(b) to prevent organised criminals, fraudsters, kleptocrats and terrorists from using companies and other corporate entities to exploit the UK's economy; and

(c) to lower the threshold for corporate criminal attribution and make it easier for UK enforcement agencies to prosecute economic crime.

Whilst some measures in ECCTA will require secondary legislation and system development by Companies House before they are introduced, other measures, such as the reformed Identification Doctrine, are already in force.[2] It is therefore important to understand the key changes implemented by ECCTA, when they come into effect and the likely impact on the business.

This guide focuses on the key developments under ECCTA which we expect will have a direct impact on corporate enforcement in the UK. These include:

(a) What constitutes fraud under ECCTA;

(b) New and additional powers for enforcement agencies;

(c) Companies House updates; and

(d) Recommended next steps.

[1] ECCTA follows on from the Economic Crime (Transparency and Enforcement) Act 2022, which sought to make it easier to identify and trace illicit wealth in money laundering and economic crimes and included the creation of the Register of Overseas Entities.

[2] See: ECCTA Implementation Timeline

What constitutes fraud under ECCTA?

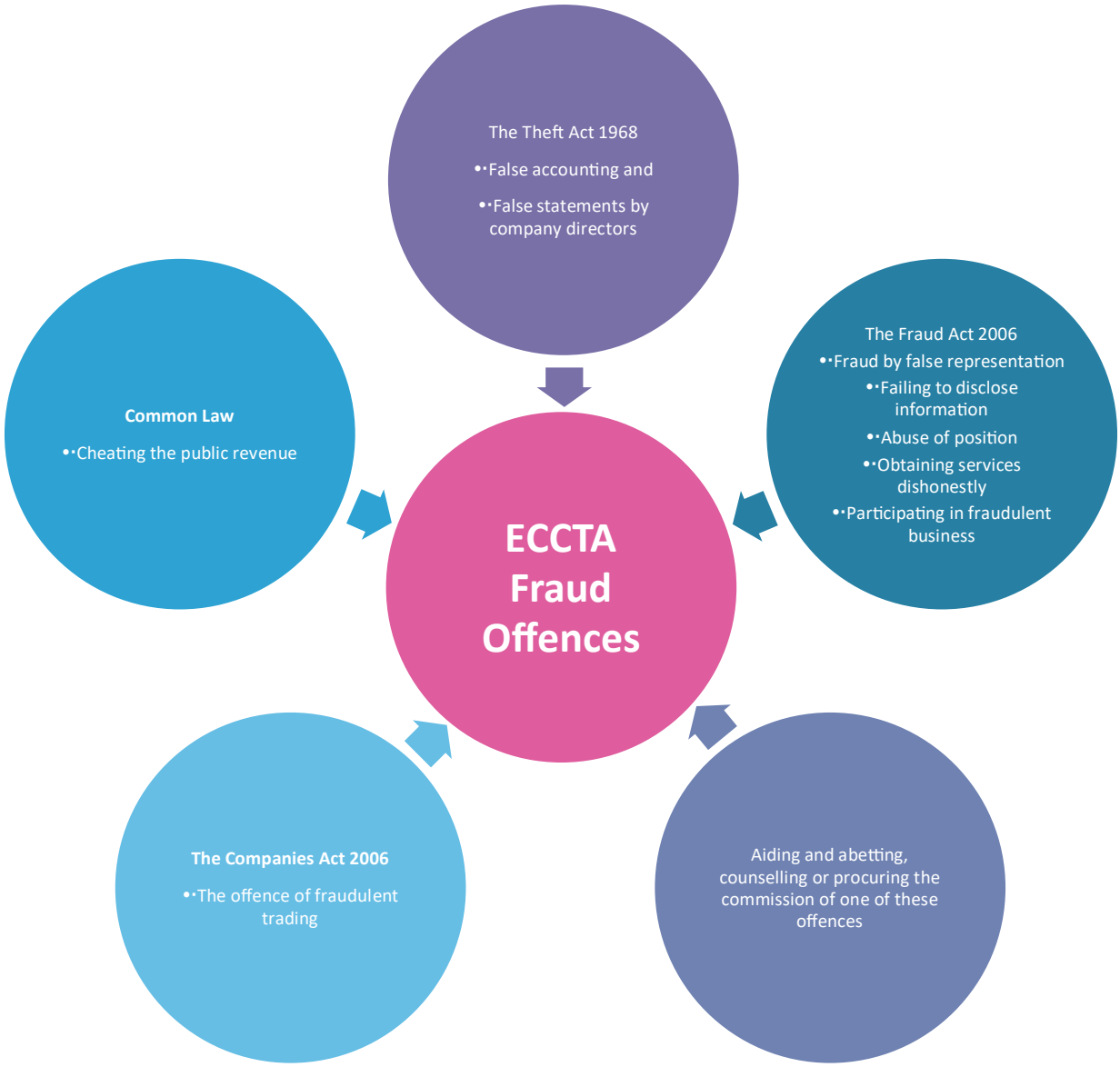
The landscape for corporates facing exposure for criminal liability for fraud on account of the actions of its employees or other entities associated with the business has expanded significantly following the introduction of ECCTA. The two noteworthy developments in this regard are the introduction of:

(a) a statutory route to the imposition of criminal liability upon companies for certain economic crime offences, including fraud, under section 196 of ECCTA (the "**amended Identification Doctrine**"); and

(b) the failure to prevent fraud offence under section 199 of ECCTA (the "**FTP Fraud offence**")

(together the "**ECCTA Corporate Offences**")

The specific fraud offences which are covered by the ECCTA Corporate Offences include:



As the above graphic shows, the fraud offences which fall to be considered under ECCTA are expansive and are therefore best assessed by focusing on the application of the ECCTA Corporate Offences to businesses.

The FTP Fraud Offence

This new offence signals a significant turning of the tide in enforcement action against companies. Previously only considered from a bribery or a tax evasion perspective, fraud is a very different, and arguably much more prevalent offence. It is expected that the introduction of the FTP Fraud offence will make it much easier for corporates to be investigated, and ultimately held accountable, for economic crime.

The FTP Fraud offence is not yet in force. Government guidance is due to be published in 2024 regarding what they consider 'reasonable prevention procedures' to be. There will then be a six-month period to enable companies to adapt their internal policies and procedures, as required, before the offence will go live.

We set out below the key considerations:

What is the new offence:	An organisation will be liable if a person associated with it commits a specified fraud offence intending to benefit the company or anyone else to whom the associate provides services on behalf of the company.
Applies to large companies and LLPs:	The offence applies to companies and incorporated public bodies qualifying as large under the Companies Act 2006, i.e., those that meet at least two of the following criteria: (a) turnover of more than £36m; (b) balance sheet total of more than £18m; (c) more than 250 employees.
Associated person:	A company will be liable if an 'associated person' commits a fraud offence for the benefit of the company. For these purposes, an associated person includes employees, agents, subsidiaries and intermediaries who perform services for or on behalf of the company.
No liability if the company is a victim:	ECCTA provides an important exemption where the company was or was intended to be a victim of the fraud offence. This means a company will not be liable where an associated person commits a fraud offence for their own benefit, rather than for the benefit of company.
Strict Liability:	A company does not have to be aware of the fraud in order to be liable. It is sufficient for a crime to be committed by an associated person for the company's benefit.
Extra-territorial effect:	Where conduct occurs abroad which would constitute fraud under UK law, or targets UK victims, A company could still be liable. Similarly, where conduct occurs in the UK, on behalf of a company based overseas, the company will still be caught.
Defence:	A statutory defence available to a company is to show that it has reasonable prevention procedures in place to prevent the fraud offences from occurring. Having recently circulated draft guidance to key stakeholders, the Government will issue guidance on what reasonable prevention procedures should look like in due course, and have indicated that the offence will go live six months after that date.
Penalties:	If a company is found liable, it faces an unlimited fine, loss in shareholder value and reputational damage, alongside the risk of civil litigation.

Although we await the publication of the final Government issued guidance on what reasonable fraud prevention measures should incorporate, we expect that a principle-based approach will be taken akin to the existing failure to prevent offences for bribery and facilitation of tax evasion. This will likely include (i) proportionate procedures, (ii) top level commitment, (iii) risk assessments, (iv) due diligence, (v) communication, including training, and (vi) monitoring and review.

The Amended Identification Doctrine

ECCTA introduces a new test for corporate liability which amends the Identification Doctrine, which is a common law test under which responsibility for wrongdoing and other acts by individuals can be attributed to a company. Under section 196 of ECCTA, an organisation will now be criminally liable when part or all of a specified economic crime is committed in the UK by a senior manager of that company or partnership.

Borrowed from the definition in the Corporate Manslaughter and Corporate Homicide Act 2007 ("**CMCHA**"), a senior manager is a person who plays a significant role in:

(a) the making of decisions about the whole or a substantial part of the activities of the organisation; or

(b) the actual managing or organising of the whole or a substantial part of those activities. The explanatory notes to the CHCHA sets out that it covers both individuals in the direct chain of management and those in strategic or compliance roles.

As such, if the senior manager is guilty of criminality, the business will also be guilty.

The amended Identification Doctrine is in effect since 26 December 2023 and will affect all companies, regardless of size. Companies should therefore prioritise identifying who their senior managers are for these purposes and assess economic crime risk falling within the scope of their authority. Consideration can then be given to how best to manage these risks.

The Serious Fraud Office (the "**SFO**")

The SFO's powers to compel individuals and companies to provide pre-investigation information have been expanded in an effort to speed up investigations. Previously, under section 2A of the Criminal Justice Act 1987, the SFO was only able to use these pre-investigation powers in relation to overseas bribery and corruption cases where it had "reasonable grounds to suspect" that such a crime had been committed.

Section 211 of ECCTA has expanded these powers to all potential SFO cases at the pre-investigative stage, including fraud, domestic bribery, and corruption. This is in effect since 15 January 2024.

At the pre-investigation stage, the SFO is heavily reliant on the voluntary provision of information. Many third-party organisations which hold useful data for potential SFO investigations generally do not provide such information absent legal compulsion on grounds of confidentiality, regulatory and / or data protection obligations. This change is expected to have a significant impact on how the SFO conducts investigations going forward as it will see an increased use of pre-investigation compulsory notices from the SFO.

The repercussions of this are expected to be felt far beyond the SFO. For third parties in receipt of such notices, there will be an increased compliance burden in reviewing and responding to them, as well as a corresponding increased burden of refreshing risk analysis across the client relationship or updated due diligence.

Importantly, the risk extends beyond the SFO's powers in a number of respects:

(a) The SFO can share information it obtains using its compulsory powers with other agencies (including overseas) via one of the information sharing gateways in s3(5) Criminal Justice Act 1987, even if those agencies do not have equivalent pre-investigation compulsory powers;

(b) The SFO may also be obliged to disclose the information to a third party that the SFO is investigating for an offence, as part of its prosecutor's duty of disclosure or as part of negotiations for a Deferred Prosecution Agreement; and

(c) Follow-on litigation and disclosure as part of related proceedings is also heightened due to the SFO's new powers.

Crypto Assets

ECCTA has also given law enforcement new powers to seize and recover cryptoassets which are the proceeds of crime or associated with illicit activity. It does so by extending existing confiscation and civil recovery powers to cryptoassets. This means that cryptoassets service providers may in future be required to follow court orders relating to the cryptoassets they hold for customers, for example to realise confiscated cryptoassets and pay the resulting sum to the court.

There are also additional powers for the police to gain access to crypto wallets and transfer cryptoassets into a wallet controlled by authorities.

National Crime Agency (the "**NCA**")

The NCA has gained greater powers to compel regulated businesses to hand over information regarding suspected money laundering and terrorist financing at an earlier stage.

The NCA's power to use Further Information Orders ("**FIOs**") was originally introduced by the Criminal Finances Act 2017. Upon receipt of a Suspicious Activity Report from someone in the regulated sector, if the NCA believes it needs to know more about potential money laundering or terrorist financing, it can apply to the magistrates court for an FIO to be served on the reporting entity or anyone in the regulated sector.

Companies House[3]

Whilst the existing remit of Companies House, per the Companies Act 2006, is predominantly to maintain a register for company information and make that information available for public inspection, the Act introduces new objectives for Companies House which aim to improve the accuracy and integrity of the information on the register and give new powers to support this role. ECCTA also contains important reforms giving Companies House a larger role to play in investigations and enforcement.

The key changes that went live on 4 March 2024 include certain powers to:

(a) Require identity verification for all new and existing registered company directors, people with significant control, and those who file on behalf of companies.

(b) Remove inaccurate or unverified material from the register and require inconsistencies to be resolved, failing which a company can be struck off.

(c) Share information in line with requests from criminal enforcement agencies.

(d) Analyse their data to prevent and detect crime.

(e) Protect personal information to protect individuals from fraud and other harms.

Also, the Registrar will, from May, have power to directly impose a financial penalty of up to £10,000 as an alternative to criminal sanctions. For example, as things stand, if a company is issued with a formal request for further information and fails to respond within 14 days, this is a criminal offence and, if prosecuted, they can face a financial penalty or an annotation of the company's record on the register to stop it misleading the public.

Under ECCTA, a new financial penalty regime is introduced that will sit alongside criminal sanctions. Once regulations are in place, the Registrar will have power to impose a financial penalty directly, as an alternative to pursuing criminal prosecution through the courts, if satisfied beyond reasonable doubt that a person has engaged in conduct amounting to a relevant offence under the Companies Act 2006.[4]

[3] Changes to UK company law - Changes to UK company law

[4] It is expected that this will come into effect in May 2024.

Recommended next steps

ECCTA Corporate Offences

From a corporate perspective, ECCTA highlights the importance of robust risk assessments and policies and procedures to identify areas of vulnerability. Further, the ability to uncover and investigate any potential wrongdoing will be crucial if companies want to avoid the reputational and financial penalties of being held accountable for the criminal acts of its senior managers.

The following steps should be considered by businesses in the short term:

(a) Conduct a risk assessment to determine fraud and corruption risk tolerances and then revise or develop policies and procedures to mitigate the risk;

(b) Conduct an exercise to determine who may reasonably be considered to be a senior manager across its operations;

(c) Conduct due diligence on all relevant connected third parties, for example, agents, suppliers and targets, including updating and incorporating appropriate contractual provisions;

(d) Large companies, who will be directly exposed to criminal liability, for smaller companies who may be compelled to certify equivalent compliance procedures when contracting with such companies, and all companies seeking to adopt best practice in their compliance procedures, once guidance on what constitutes 'reasonable procedures' for the failure to prevent fraud defence is published, prepare suitable policies and procedures;

(e) Develop and deliver bespoke fraud prevention training; and

(f) Develop a crisis response protocol in the event there is an allegation of failing to prevent fraud, outlining the process for investigation through to remediation.

Companies House

Most of the ECCTA provisions enhancing the powers of Companies House to tackle economic crime and enhance corporate transparency came into force on 4 March 2024. If you have yet to take any steps in response, the following points should be prioritised and the next round of changes at Companies House should be timetabled:

(a) Make sure information presented on the Registry is consistent with your local statutory registers. If any changes take place, adhere to the relevant filing deadlines to avoid fees;

(b) If you use the Companies House Webfiling platform, consider who has access to the company authentication codes in order to submit these filings. Check these individuals are suitable, of appropriate seniority and authorised to file on behalf of the company;

(c) Provide a full registered office address as PO boxes are no long permitted. A company email address is also required to be provided on incorporation or on the filing date of the next confirmation statement;

(d) Confirmation should be given that a company is being formed for a lawful reason and that the intended business activities are lawful; and

(e) Later this year, Companies House will:

(i) implement a platform which allows it to verify the identity of persons listed on the register such as Directors, Persons with Significant Control and members of LLP's. Failure to comply with the verification process can amount to a criminal offence and lead to disqualification. In anticipation of this, companies should obtain copies of the necessary identification documents, such as passports and proof of address; and

(ii) abolish certain local registers, reducing the administrative burden and providing a one-stop shop at Companies House for statutory registers going forward. To prepare for this change, make sure the information you currently have on file is up-to-date and consistent with the corporate structure.

ECCTA Implementation Timeline