trowers & hamlins

—— trowers.com

Fortify your business against fraud

Progress on the ECCTA and implementing fraud prevention procedures

Key contacts

Elizabeth Mulley
Managing Associate

+44 (0)121 214 8864
EMulley@trowers.com

Amy-Rose Hayden
Senior Associate

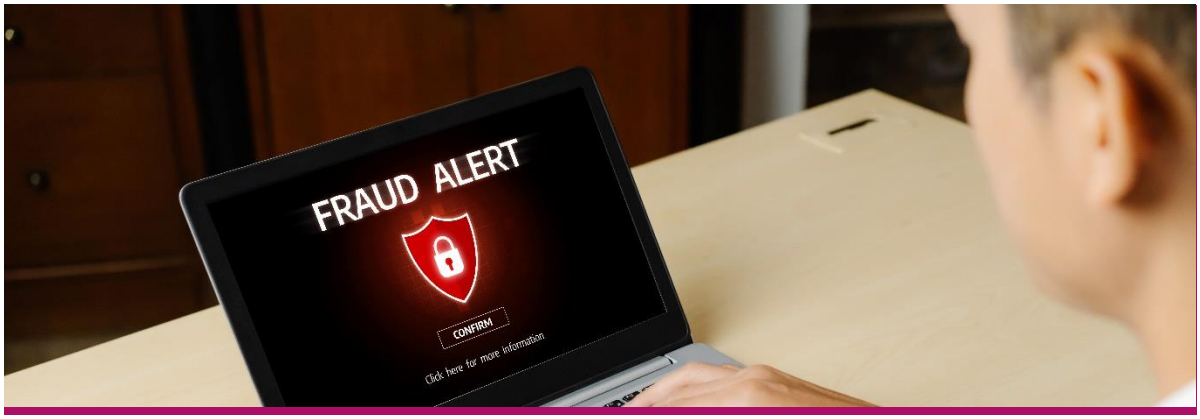
+44 (0)121 203 5672
AHayden@trowers.com

July 2024 ——

The threat of economic crime continues to grow. Fraud is the most common crime, accounting for 40% of all offences in England and Wales[1].

Fortunately, the government is listening and fraud is now firmly on the agenda. In the last year in particular we have seen the UK take significant action. There has been a welcome introduction of measures, including legislation, designed to help cut crime, protect our national security, and support the UK's legitimate economic growth and competitiveness[2].

The first measures under the Economic Crime and Corporate Transparency Act (**ECCTA**) came into force on 4 March 2024, with over 50 or more statutory instruments needed to underpin and implement these reforms. However, as ever, legislation is not enough to protect businesses from fraud. This article covers some of the key legislative changes as a result of the ECCTA and their initial results published by the Department for Business & Trade (**DfB&T**), together with key takeaways on how organisations can enhance their fraud prevention measures.



Key changes under ECCTA

Many fraudulent transactions are conducted through corporate entities. The ECCTA seeks to deliver a number of measures to tackle fraud and economic crime and improve the transparency within corporate entities, including:

- Reforms to Companies House such as identity verification checks for all new and existing company directors, persons with significant control and those delivering documents to the Registrar, broadening the Registrar's powers over company creation and enforcement powers and improving financial information;

- Strengthening anti-money laundering powers to give businesses more confidence to share information for the purposes of preventing, investigating or detecting crime by disapplying civil liability for breaches of confidentiality, and enabling proactive intelligence gathering by law enforcement and focusing resources on high value activity;

[1] National Crime Agency
[2] Economic Crime Plan 2, 2023 - 2026

- Additional powers to seize and recover suspected criminal cryptoassets to law enforcement in the form of criminal confiscation and civil recovery pursuant to Parts 2 to 5 of the Proceeds of Crime Act 2002 (**POCA**); and

- Reforms to prevent the abuse of limited partnerships by tightening registration requirements whilst increasing transparency and requiring limited partnerships to maintain a connection to the UK.

Corporate liability

In addition to the above measures, two significant reforms have been made in the area of corporate criminal liability through the ECCTA to enhance the legal framework targeting fraud carried out through corporate entities.

Failure to prevent fraud offence

The government has introduced the new offence of a failure to prevent fraud. The purpose of the offence is to discourage organisations from turning a blind eye to fraud committed by employees or agents that is inadvertently benefiting it. The offence is also designed with the aim of driving businesses and organisations to closely monitor their existing fraud practice and policies.

Under the new failure to prevent fraud offence, the government explains a relevant body will be liable where a fraud offence specified under the ECCTA, is committed by an “associated person” such as an employee or agent, for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place.

A relevant body is defined to mean a body corporate or a partnership, wherever incorporated or formed. This means the obligation will equally apply to large corporations and SMEs for uniformity and consistency in fraud prevention practices. It is also important to note if an employee commits fraud under UK law, or targets UK victims, their employer could be prosecuted, even if the organisation (and the employee) is based overseas.

There is a defence for a corporate if it can prove that it had reasonable procedures in place, or that it is reasonable to have none. The government will publish guidance on providing organisations with more information on this before the new offence comes into force (which is expected to be by late 2024 / early 2025).

If convicted, an organisation can receive an unlimited fine. There will be no limit to the circumstances the court can take into account when deciding the appropriate level of fine.

Reformed identification doctrine

Section 196 of the ECCTA creates a statutory route for liability on a corporation where a 'senior manager' commits a relevant economic offence whilst acting with the (actual or apparent) scope of their authority of that corporation. For the first time in over 50 years, the 'identification doctrine' has been reformed to codify and widen the position that held a company can be liable if it can be proven that the "*directing mind and will*" of the company committed the offence, which was based on longstanding case law. In addition, it will apply to virtually all corporates and partnership, not limited to a certain size or turnover.

A 'senior manager' for the purposes of this offence means an individual who plays a significant role in:

a) the making of decisions about how the whole or a substantial part of the organisation's activities are to be managed or organised; or

b) the actual managing or organising of the whole or a substantial part of those activities.

As such, job title or role is not as important as what that individual does in practice. It also seems likely that this would include individuals not employed by the company, such as consultants.

In terms of a qualifying economic offence, this will be an act constituting, but not limited to, the economic crimes listed in Schedule 12 of the ECCTA such as cheating the public revenue; conspiracy to defraud; theft; false accounting; false statements by company directors; fraud and VAT offences; and certain offences under the Financial Services and Markets Act 2000, Financial Services Act 2012, Bribery Act 2010, POCA, and the Terrorism Act 2000.

Again, an organisation convicted will be subject to an unlimited fine, as well as disbarment from public contracts (under the Procurement Act 2023). As such corporate liability will be applicable to the makeup of modern corporations and deter instances where senior managers use authority granted under the company to commit economic crimes. This reform came into force on 26 December 2023.

Initial progress report

The government has agreed to make a statutory commitment to report on the progress of the reforms, with the DfB&T's first progress report (the **Progress Report**) having been released and further reports to follow every 12 months until 2030. The Progress Report sets out some of the achievements so far and next steps.

Companies House and limited partnerships

The first phase of implementation was delivered on 4 March 2024, encompassing the systems, process and organisational change needed to operate the new Companies House Registrars objectives and powers and new legal requirements for companies.

Cleansing the companies register has been an immediate priority. From 4 March to 1 April 2024, Companies House has:

- commenced the process to remove names and addresses used without consent. This includes removals of People of Significant Control (PSC) and shareholders. Previously those wishing to have their details removed would have had to apply to the courts;
- removed 4,000 registered office addresses;
- removed 2,100 officer addresses and 2,300 PSC addresses;
- redacted 3,600 incorporation documents to remove personal data used without consent;
- removed 1,250 documents from the register, including 800 false mortgage satisfaction filings which would have previously required a court order; and
- contacted 3,800 companies with PO Boxes as their registered office address, to make them aware that this would no longer be legally compliant and requiring them to provide an alternative appropriate address. As of 1 April 2024, the number of companies on the register using a PO box has reduced to 1,900.

There will also be new powers for Companies House to challenge company names where they may be intended to facilitate fraud, comprised of or contain computer code, or are likely to give the false impression that it is connected to a foreign government or international organisation. If a company is directed to change its name, and fails to within 28 days, not only is an offence committed but Companies House will be able to determine a new name.

To ensure momentum is maintained, Companies House has also overhauled its fees and funding model. From 1 May 2024 Companies House amended company incorporation and registration fees to bring them in line with the costs of providing services, together with recovering the costs of its new powers as a result of the ECCTA such as funding the cost of additional criminal referrals to the Insolvency Service.

Official statistics on companies register activities will be released to enable monitoring of the register as to the implementation of the ECCTA. On 27 June 2024 the official statistics on the register activities from April 2023 to March 2024 was released (the **Official Statistics**). The Official Statistics confirm that the number of companies on the total register reached 5,350,759 (by 31 March 2024), increasing 4.6% compared to FYE 2023.

It is envisaged that, subject to the Parliamentary timetable and passage of secondary legislation, the introduction of a registration process for third party agents to become Authorised Corporate Service Providers will be in Winter 2024, and the ability to perform identity verification will commence during the first half of 2025, with a full implementation timetable to be published shortly. These reforms seek to make anonymous filings harder and discourage those wishing to conceal ownership through convoluted structures. Similar reforms will be applied to limited partnerships and are expected to come into force during 2026.

Whilst a step in the right direction, there are still a number of issues to be addressed in order to reduce the risk of Companies House being used to facilitate fraudulent activity. Our previous article on this topic discussed the appeal of Companies House to criminals who are able to pay low registration fees and use complex structures to enable money laundering.

In particular, fraudsters may use real stolen identities to bypass verification checks to set up companies. Graham Barrow, Director at the Dark Money Files Ltd, discussed his investigations on this topic at the Midlands Fraud Forum on 27 June 2024. Mr Barrow explained how fraudsters take advantage of the fact that firms could be registered to any address in the UK. They therefore register companies with near identical names to existing establishments and use real stolen identities to install as the company's director(s), and are then able to obtain access to bank accounts. Filing false documents will be a criminal offence pursuant to the ECCTA, however policing over 5 million companies will require significant resource and will take time. It will certainly not be a quick fix but will assist in deterring or apprehending some fraudsters.

Register of overseas entities

The Register of Overseas Entities (**ROE**) was introduced via the Economic Crime (Transparency and Enforcement) Act and came into force in the UK on 1 August 2022. The ROE has seen 30,000 overseas entities registered (out of an estimated 32,000 in scope) since its launch.

The ECCTA makes amendments to previous legislation that will bring the requirements for ROE in line with new requirements for companies, such as identity verification. It also includes provisions in respect of additional information on trusts and beneficiaries including access to trust data and the introduction of an associated protection regime.

The ECCTA gives Companies House new powers to improve the integrity of the register and the transparency of overseas entities. Guidance to ensure compliance was published and updated on 20 May 2024. Any overseas entities that fail to:

(i) comply with the duty to update the register;

(ii) register by the end of the transitional period / if required by the Secretary of State or Department for Business and Trade;

(iii) comply with notices;

(iv) resolve inconsistencies in the register;

(v) commits a (aggravated) false filing offence;

(vi) disposed of land between 28 February 2022 and the end of the transitional period; or

(vii) commits an offence under other legislation

may face restrictions on selling, transferring, leasing or raising charges against property or land. An Overseas Entity ID will also be required to buy new UK property or land. Enforcement action may include civil financial penalties (which could be at a fixed rate, daily rate or a combination of both) and / or prosecution of criminal activity. Resources towards enforcement action will be prioritised where offences have been persistent, repeated or there has been wilful non-compliance. In order to impose a civil financial penalty the standard to meet is that an offence has been committed beyond reasonable doubt. Entities may be referred to the Insolvency Service or other law enforcement agencies to be considered for prosecution.

Partnership working

Another important concern to authorities and companies alike is in respect of data sharing and confidentiality. Companies House has now been afforded greater ability to share data with law enforcement, other government bodies and private sectors including the anti-money laundering regulated sectors. This means that feedback loops can more effectively establish suspicious activity, internal intelligence is developed to identify threats and provide faster support to investigations in tackling fraudulent activity.

The Report also notes that the Insolvency Service is a key partner in these reforms, with important steps already having been taken. For example, a Memorandum of Understanding with Companies House has been established to enable funding to flow into more complex investigation and prosecutions. As a result, it is planned that the Insolvency Service will implement a process to allow referrals from Companies House in relation to breaches of the ECCTA and in time quantify these metrics.

What can you do?

The ECCTA reforms will make it more likely that businesses can be successfully prosecuted and / or fined in relation to economic crime as a result of the actions of its employees or agents. It is therefore important that businesses act now in order to prepare. In particular, an organisation accused of failing to prevent fraud is likely to be required to demonstrate that it had reasonable procedures in place, or if it did not, that it was reasonable not to have such procedures. Based on current draft guidance, the defence will take a similar form to the 'adequate procedures' defence for a failure to prevent bribery. This sets out six principles:

proportionate procedures; top-level commitment; risk assessment (documented); due diligence; communication (including training); and monitoring and review. Further, it seems likely that parent companies will need to take action to implement group level policies and training to prevent fraud in their subsidiary companies.

There are a number of helpful steps that all organisations can take in order to ensure compliance with the ECCTA taking into account the current draft guidance on the defence for a failure to prevent fraud and the extension of corporate liability via the identification doctrine, as well as enhancing fraud and economic crime prevention controls:

- **Proportionate procedures –** this means that an organisation's procedures to prevent fraud and economic crime by the persons associated with it are proportionate to the risks it faces, as well as the nature and scale of its activities. Developing a strategy detailing controls and procedures is essential in fraud prevention and detection. Identifying gaps and understanding which controls can best alleviate the risks as a result is a continuous process. Appropriate controls can include physical controls such as access to assets, technical controls such as authentication and authorisation measures, reconciliation exercises and segregation of duties. For example, having approval processes in place that strike the balance between ensuring no individuals can process payments without another party verifying the sums whilst making timely payments to vendors.

- **Top-level commitment –** a fraud prevention culture has to start from the top. Communication and messaging from the organisation's management to demonstrate a zero tolerance policy to fraud and economic crime is essential to ensure employees are equally engaged to ensure common purpose. This could include involvement in critical decision making and risk assessments where possible, hosting training, sharing prevention policies and issuing a formal statement / commitment. Unlike the failure to prevent fraud offence, the identification doctrine has no statutory defence to rely on, therefore identifying the individuals that may fall under the 'senior manager' definition is important, particularly for corporates with complex structures and subsidiaries. The commitment and compliance of senior management will be imperative to organisations avoiding penalties for economic crimes committed by senior management.

- **Risk assessments –** undertaking a company-wide risk assessment to assess internal and external fraud risks is a critical first step for any organisation when putting in place and evaluating existing anti-fraud procedures. The appropriate individual / working group conducting the internal risk assessment will need to seek input from important functions within the business, such as finance, IT, HR, legal, with oversight by senior management. External risks such as third party suppliers, customers and contractors will need to be carefully assessed too, with contracts including audit and request for information rights in place. The risk assessment and decisions made will need to be documented, supported by evidence, and reviewed at regular intervals. Ultimately a risk assessment is required to reduce the risk of a fraud happening, as well as giving the business the tools to defend allegations.

- **Due diligence** – an organisation that has good corporate governance will encourage due diligence procedures in respect of persons or organisations that performs services for or on its behalf. When onboarding any third party suppliers or contractors, appropriate checks, systems and controls must be in place to mitigate the risk of fraud and economic crime in an organisation's supply chain. Due diligence conducted using

a risk-based approach is practical; in higher risk situations due diligence could involve investigations, interrogative enquiries and / or general research on the business and associated persons.

- **Communication (including training)** – internal and external communication and education can be an effective deterrent to those intending to undertake fraudulent behaviour. All organisations should have an appropriate way that employees, agents and / or third parties can report a fraud in a discreet manner. Not only does this provide a way for individuals to raise any concerns, it also serves to promote a zero-tolerance approach to fraud and economic crime. As well as reporting processes, there should be employees charged with direct responsibility for combating fraud and economic crime. Employees can be an organisation's greatest strength to mitigate against the risks of fraud. Larger organisations and businesses in certain sectors may have internal audit teams, Money Laundering Reporting Officers or those who assist management in ensuring compliance, whereas smaller businesses may require the board or senior management to oversee prevention. In addition, having comprehensive and robust policies and controls in place is only helpful if employees know where to look for them, understand them and talk about them. Educating senior management, employees and consultants through internal communication and training programmes is crucial. Workshops or risk assessment exercises in particular are helpful to ingrain consistent anti-fraud behaviours and raise awareness.

- **Monitoring and review –** appraisals and regular monitoring are crucial to ensure that any changes to the fraud and economic crime risk profile of an organisation are considered, with policies and procedures updated as appropriate. Testing and evaluating the procedures in place, for example by way of periodic reviews or reports to management, will assist in ensuring effectiveness of prevention measures. Organisations should ensure that they have in place a tried and tested response strategy if fraudulent activity is reported / identified which details who is responsible for dealing with these matters, who needs to be informed (regulatory bodies, lawyers, stakeholders), and setting out parameters for investigations.

- **Updates to Companies House** – the ECCTA introduces a range of compliance requirements for the information to be notified to Companies House. For both companies and limited partnerships, up to date and accurate information will need to be supplied. There are also additional identity verification requirements for all new and existing directors, PSCs and anyone delivering documents to Companies House, which will mean that these individuals will need to be prepared to undertake the verification process. Companies with complex structures or group companies will also need to consider any changes that may be required in order to ensure any 'layering' is removed.

Organisations will need to keep abreast of the latest guidance. The campaign site for changes to UK company law is a helpful hub in order to understand the upcoming amendments and compliance required of new and existing directors, people with significant control and those filing on behalf of a company.

How we can help

No business is the same, with different governance structures, operating environments and assets, and each will require a different approach and considerations. It can take weeks or even months to undertake risk assessments and implement new procedures. Whilst a

proportion will already have a fraud prevention framework in place, now is the time to be reviewing that framework and considering how the implemented and upcoming changes will affect your organisation.

Our fraud and risk management experts are on hand to assist you in navigating through the ECCTA reforms and bolstering your internal measures to mitigate against fraud and economic crime. We can work with you to take proactive steps in fraud prevention, in drafting and reviewing policies, conducting fraud risk assessments and providing training to boards and employees. We are also on-hand in the event that an incident occurs, gathering evidence, conducting in-depth investigations and communicating with stakeholders, including regulators, throughout, as well as taking swift action to recover misappropriated assets.

Contacts

Jamie De Souza
Partner
Dispute Resolution and Litigation
+44 (0)121 214 8847
JDeSouza@trowers.com

Helen Briant
Partner
Dispute Resolution and Litigation
+44 (0)121 214 8867
HBriant@trowers.com

Elizabeth Mulley
Managing Associate
Dispute Resolution and Litigation
+44 (0)121 214 8864
EMulley@trowers.com

Amy-Rose Hayden
Senior Associate
Dispute Resolution and Litigation
+44 (0)121 203 5672
AHayden@trowers.com

Emily Sharples
Senior Associate
Dispute Resolution and Litigation
+44 (0)121 214 8874
ESharples@trowers.com

Meera Solanki
Associate
Dispute Resolution and Litigation
+44 (0)121 203 5646
MSolanki@trowers.com

Hannah Jakeman
Associate
Dispute Resolution and Litigation
+44 (0)121 214 8875
HJakeman@trowers.com

Rachel Storey
Associate
Dispute Resolution and Litigation
+44 (0)121 203 5625
RStorey@trowers.com