Building a better working world

FS insights

The impact of upcoming UK corporate fraud legislation for financial services

Introduction

41% of all crime in the UK is due to fraud
UK government (September 2022)[1]

High levels of fraud in the UK have led to increased scrutiny by legislators, regulators, investors, and broader society. For example:

- The new Economic Crime and Corporate Transparency Bill (ECCTB), which introduces a new corporate "failure to prevent" fraud offence
- The Financial Conduct Authority (FCA) conducting multi-firm reviews into firms' anti-fraud systems and controls, and firms' controls to detect and prevent money mules
- The Payment Systems Regulator's (PSR) policy on mandatory reimbursement of authorised push payment (APP) scam losses, empowered by the Financial Services and Markets Bill (which received Royal Assent on 29 June 2023)

This article explores the new corporate failure to prevent fraud offence in more detail, together with recommended actions that organisations should be undertaking now to prepare for their implementation.

The focus of the FCA and PSR is protecting financial institutions' customers from fraud (rather than directly addressing fraud committed by corporations) and is the subject of separate EY thought leadership.

1. "Failure to prevent fraud offence", UK government, gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/factsheet-failure-to-prevent-fraud-offence

The criminal offence of failure to prevent fraud

> The UK government has introduced legislation through the ECCTB that will make a company criminally liable if it fails to prevent a fraudulent act perpetrated by one of its associated persons.[2]

To be in scope of the bill, the fraud must have been committed for the benefit of the company. The only defence permitted under the law would be that the company had reasonable procedures in place to prevent fraud (and could demonstrate this). This aligns with similar corporate "failure to prevent" offences previously introduced by UK legislation, such as the Bribery Act 2010 (for failing to prevent bribery) and the Corporate Criminal Offence 2017 (for failing to prevent the facilitation of tax evasion).

The purpose of the legislation is twofold. Firstly, holding organisations accountable through prosecutions will force them to take responsibility for the behaviour of their employees and agents, leading to more ethical behaviour in the workforce. Secondly, allowing a defence of possessing effective fraud prevention procedures will drive a cultural change towards improved anti-fraud systems.

Timing of the new legislation

We anticipate that this legislation will come into force in Q4 2024, with guidance from the UK government on reasonable procedures being published ahead of that.

Scope of the new failure to prevent offence

The offence will apply to all large bodies and corporate partnerships as defined in Companies Act 2006. Companies meeting any two out of the following criteria will be in scope:

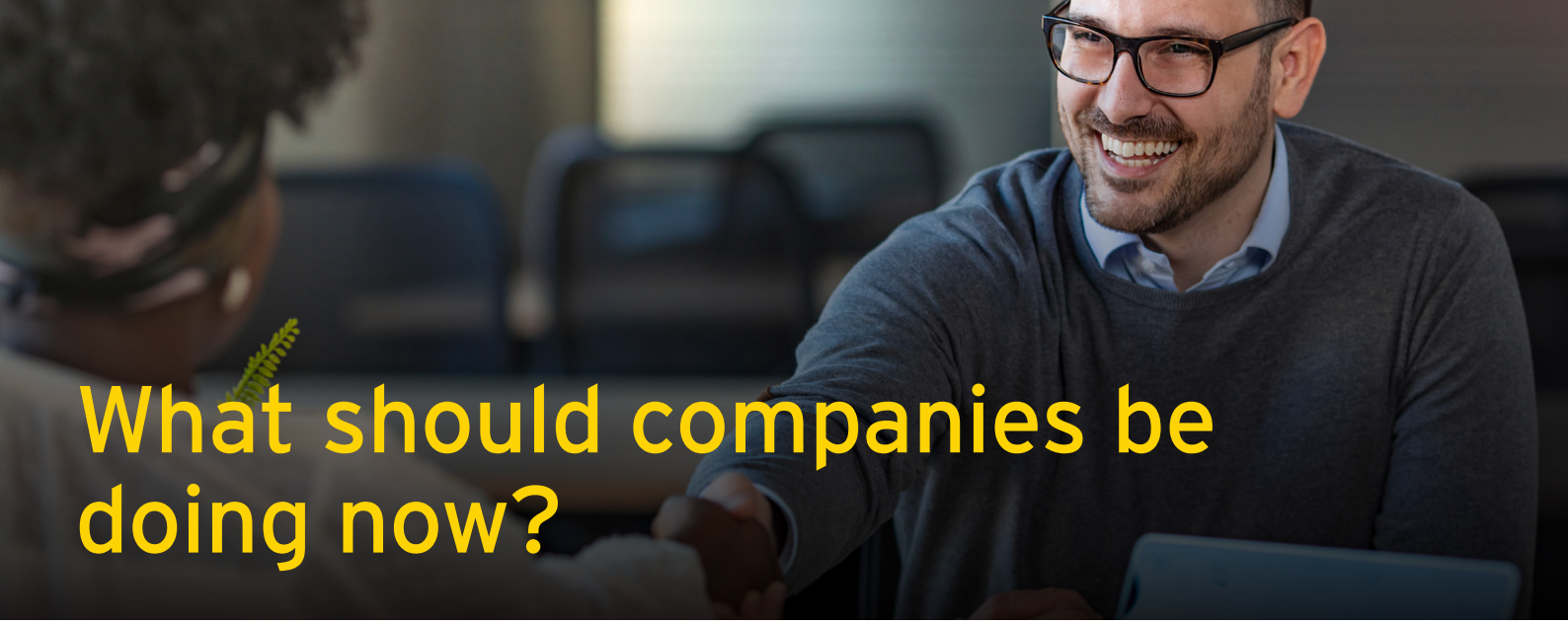
1. Having more than 250 employees
2. Generating over £36m in turnover
3. Holding more than £18m in total assets

The UK government has stated that **"if an employee commits fraud under UK law, or targeting UK victims, their employer could be prosecuted, even if the organisation (and the employee) are based overseas."** Therefore, the offence could impact global organisations without UK presence or operations. Again, this would be consistent with the scope of the Bribery Act 2010 and the Corporate Criminal Offence 2017.

The proposed offence will apply to a wide range of fraudulent activity, covering multiple areas of a company's workforce. Some examples include:

- Fraud by false representation, such as mis-selling a product to a customer
- False statements by company directors, such as misrepresenting the financial position of the company to shareholders
- False accounting, such as delaying the recognition of an asset revaluation until the next year
- Cheating public revenue, for example failing to declare the correct income on tax returns

2. An associated person is defined as an employee or agent acting on behalf of the company.



What should companies be doing now?

> In light of the new legislation, companies should consider the potential scope of impact to their organisation – focusing on how these new rules may affect their business and how they can prepare.

Now

Review existing policies and procedures

Given the breadth of the new legislation and the rapidly evolving nature of fraud, organisations should assess whether their existing definitions of internal and external fraud are adequate. For example, do they include "greenwashing" or improper use of customer datasets, whether they cover the actions of associated persons, what impact this might have on associated policies and procedures (such as whistleblowing) and therefore what changes need to be made to these policies and procedures? When an assessment is complete and plan of action is agreed upon, the organisation should then effectively communicate all changes to relevant staff and third parties. This will allow organisations to evidence effective fraud controls as part of a future defence against the new offence.

Establish governance

If not already defined, companies should consider where the overall ownership of anti-fraud function resides within their organisational structure and if this is optimal. This should include identifying owners of all fraud risks including internal and external fraud, and defining which types of fraud are in scope of the new legislation. Clear and appropriate ownership allows fraud initiatives to be executed efficiently and given the attention and sponsorship they require, and that fraud issues are dealt with promptly and effectively. Ownership and responsibilities should be clearly documented in terms of reference for committees and working groups, including where there is delegated authority from the board. Well-defined ownership will also simplify and expediate other anti-fraud initiatives and will help demonstrate management's oversight and commitment to preventing fraud.

Fraud framework readiness assessment

By performing a detailed review of their fraud framework, companies can identify gaps and development areas as well as create a roadmap. This should include gap assessment of anti-fraud systems and controls against current threats and proactivel horizon scans for future fraud risks. An effective fraud framework will form a key part of a future defence against the offence.

Next

Planning Workshops

By conducting strategy workshops on the potential outputs of the offence, internal stakeholders can be educated on the new legislation. The role of stakeholders and their responsibilities for ownership of processes in the new regime can be defined and agreed upon.

Establish a regular programme to monitor emerging fraud methodology and risks

Monitoring internally generated management information (MI) and loss data will help to identify new trends already affecting the organisation. Regular engagement with industry bodies, regulators and other external stakeholders enables businesses to discuss the impact of new technologies such as generative AI, or market developments, such as the spread of faster payments. Given the cross-border nature of fraud, these activities should take place in all the major jurisdictions in which an organisation operates (or plans to).

Perform/update an existing fraud risk assessment (FRA)

If not already part of business-as-usual operations, companies should begin conducting FRAs to identify higher risk areas and control gaps in their fraud framework. Performing this activity effectively and regularly will reduce the likelihood that a company will fall foul of the offence. Documenting the activity and results will help the company in any future defence.

Beyond

Identify synergies with other risk domains

Organisations can identify other functions in the business which have controls that are relevant to preventing and detecting fraud by the organisation's employees or agents. This could include functions like human resource (HR), cybersecurity, physical security and trader surveillance. These functions may have data which can be used to enhance the effectiveness of fraud detection and prevention systems.

How EY teams can help

- **Light touch health check:** EY teams can perform a desktop review of key fraud documentation and interviews with key stakeholders, providing market insights analysis against peers and leading industry practice. The health check will provide observations and recommendations for alignment with the market insights analysis results.
- **In depth readiness assessment:** EY teams can perform a current state assessment of the existing fraud framework and then work with stakeholders to define the future fraud operating model aligned with market insights and leading best practice.
- **Lead or facilitate planning workshops:** EY teams can leverage its industry knowledge to conduct strategy workshops which cover the legislation as well as the PSR and FCA fraud initiatives. We can also provide employees with training on the new legislation and regulations, as well as offer guidance on determining the roles and responsibilities for relevant processes.
- **FRAs:** We can assist EY clients in designing and performing FRAs, covering a range of risk areas and fraud typologies across the business.

Contact us for more details of how we can support you with this.

Key contacts

For further information, please contact the financial crime & forensics team.

Hemen Shah
Partner,
Financial Crime & Forensics, EY LLP

T: +44 20 795 18257
E: hshah2@uk.ey.com

Ted Rugman
Director,
Financial Crime & Forensics, EY LLP

T: +44 20 7951 4331
E: trugman@uk.ey.com

James Good
Senior Manager,
Financial Crime & Forensics, EY LLP

T: +44 20 795 18027
E: jgood@uk.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 011008-23Gbl
ED None

UKC-031521.indd (UK) 11/23.
Artwork by Creative UK.

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com