Published on *The National Law Review* https://www.natlawreview.com

Why Corporates are Now More Likely to Face Criminal Prosecution for the Actions of Their Employees

Article By:

Dylan G. Moses

Michael E. Ruck

Rosie Naylor

Joseph K. Skilton

SIGNIFICANT EXPANSION TO CORPORATE CRIMINAL LIABILITY BECOMES LAW IN THE UNITED KINGDOM

On 26 October 2023, the Economic Crime and Corporate Transparency Act (the Act) became law. Under the Act, corporations will become criminally liable for the acts of their "senior managers" as well as for any failure to prevent their employees and associates from committing fraud. Together, these two reforms will significantly expand the exposure of corporates to criminal prosecution. This briefing explains these reforms, analyses their impact, and considers what corporates need to do to comply.

RATIONALE FOR REFORM

Presently there are three ways corporates can become criminally liable: (a) by the identification doctrine, (b) through vicarious and strict liability offences, or (c) through specific offences created by parliament, such as corporate manslaughter or failure to prevent bribery.

However, there has been growing momentum to reform the corporate criminal liability regime in the United Kingdom. This momentum principally derives from a sequential three-factor problem: difficulty in bringing corporate criminal prosecutions has led to poor enforcement outcomes which have created an accountability “loophole” whereby large multi-national companies with complex and diffuse structures and hierarchies are not prosecuted. Behind each of these factors, though, is the underperformance and underfunding of UK prosecutors. In particular, the Serious Fraud Office (SFO) had its funding reduced after the global financial crisis and has faced many high-profile prosecution failings.

As a result, the impetus for reform was present and two landmark reforms which expand the identification doctrine and introduce a new criminal offence have been enacted.

EXPANDED IDENTIFICATION DOCTRINE

The Reform

The identification doctrine was developed to allow corporates to be criminally liable in the same way natural persons are. It transposes the mind and body of a company's controlling officers to the company itself. Specifically, the doctrine provides that a corporate entity can be held criminally liable for the actions of an individual if that individual was the "directing mind and will" of the corporate entity.

However, the concept of a "directing mind and will" has been criticised as too narrow. Especially following the collapse of a recent SFO case when the High Court held that a CEO and CFO did not have sufficient authority to be the corporate's directing mind and will.

Under the Act, the identification doctrine is placed on a statutory footing and expanded so that corporates can be held criminally liable for the actions of an individual if that individual was a "senior manager" of the corporate and commits a relevant offence acting within the actual or apparent scope of their authority.[1]

While “actual or apparent scope of authority” is not defined under the Act, there is a definition for “senior manager”:

“Senior Manager means an individual who plays a significant role in—

(a) the making of decisions about how the whole or a substantial part of the activities of the body corporate or (as the case may be) partnership are to be managed or organised, or

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

In short, this will require corporates to carefully consider who may fall within this definition. This will require an assessment of an individual’s role, responsibilities, and level of influence within an organisation rather than their job title. It should also be noted that the definition is not limited to the meaning given to senior manager under the Financial Conduct Authority and Prudential Regulation Authority Senior Managers Regime.

The definition of “senior manager” will inevitably be an area that is tested by future prosecutions under the newly expanded doctrine.

In addition, this reform only applies to the committal of a "relevant offence" by the senior manager. A long list of relevant offences covering various economic crimes including bribery, fraud, money laundering, sanctions, tax evasion, terrorism, false accounting, and financial services offences is provided at schedule 12 of the Act. The government plans to increase the scope of "relevant offence" in the future to cover all criminal offences.

Impact on Businesses

The expansion to the identification doctrine does not come into force until 26 December 2023. Therefore, from Boxing Day, corporates will face an increased risk of prosecution as a result of this reform. In the past, UK prosecutors have often appeared hapless at prosecuting large corporates; these companies will now be targets for new prosecutions.

Recommended Compliance Actions

Due to the expanded identification doctrine, we recommend corporates engage in the following compliance actions:

- Identify those in your business who fall under the Act's definition of "senior manager." This definition may be interpreted widely by UK prosecuting agencies. Corporates should not interpret this too narrowly before

it has been tested in court.
- Provide updated training to your “senior managers” on economic crime risks, applicable procedures, and the new criminal liabilities posed by the Act’s reforms.
- Review your compliance programmes and risk assessments to ensure they are proportionate to the increased risk of prosecution.

NEW FAILURE TO PREVENT (FTP) FRAUD OFFENCE

The Reform

The Act also introduces a new criminal offence of FTP fraud.[2] A corporate commits the FTP fraud offence when their employee or associate (this means a person who performs services for or on behalf of the corporate) commits a relevant fraud offence intending to benefit the corporate. A list of the relevant fraud offences is included in schedule 13 of the Act.[3]

The offence only applies to “large organisations” and their subsidiaries. “Large organisations” are corporates who satisfy two of the following three criteria:

- > 250 employees
- > £36 million turnover
- > £18 million total assets

Under the Act, the corporate has a complete defence if, at the time the fraud offence was committed by the employee or associate, the corporate had reasonable fraud prevention procedures in place.

The maximum penalty if found guilty of FTP fraud is an unlimited fine.

Impact on Businesses

By introducing a defence of having “reasonable fraud prevention procedures” this new reform effectively criminalises large corporates who have inadequate fraud prevention procedures in place. Therefore, the intended effect of the Act is to force large corporates into improving their fraud prevention procedures via the threat of criminal prosecution.

The government has estimated the one-time cost of compliance for large UK corporates collectively is £500 million. The annual recurrent cost for these businesses collectively is estimated to be £60 million.[4]

The new offence is not yet in force. Only once the government has issued guidance on what constitutes “reasonable fraud prevention procedures” will the offence

become live.

However, this guidance is likely to be based on the same model used for equivalent guidance issued on the existing offences of failure to prevent bribery and failure to prevent tax evasion.

Recommended Compliance Actions

Corporates falling within the scope of the new offence should review and, where required, improve their fraud prevention procedures based on the “six principles.” These six principles form the basis of government guidance on reasonable bribery and tax evasion procedures and are likely to form the basis of the government’s future guidance on fraud procedures. The six principles are as follows:

Proportionate Procedures

The extent and type of your procedures must match the fraud risks, as well as the specific nature, scale, and complexity of your organisation’s activities.

Top-Level Commitment

The highest levels of management within your organisation should be involved in communicating and making decisions

on developing procedures which exhibit zero tolerance for fraud.

Risk Assessment

Periodic, informed, and documented assessments of exposure to potential internal and external risks of fraud being committed on your organisation’s behalf by persons associated with it.

Due Diligence

Perform due diligence in respect of persons who do or will perform services for or on behalf of your organisation. The extent of due diligence applied for each person should be based on their fraud risk level.

Communication

Use internal and external communication and training to ensure your fraud procedures are understood. Establish secure communication channels so individuals can raise concerns.

Monitor and Review

Implement systems to monitor and review fraud prevention procedures to measure efficacy and make improvements

where necessary (e.g., through periodic reports, third-party verification, or staff surveys).

[1] s.196 Economic Crime and Corporate Transparency Act 2023.

[2] s.199 Economic Crime and Corporate Transparency Act 2023.

[3] These are: fraud by false representation (section 2, Fraud Act 2006), fraud by failing to disclose information (section 3, Fraud Act 2006), fraud by abuse of position (section 4, Fraud Act 2006), obtaining services dishonestly (section 11, Fraud Act 2006), participation in a fraudulent business (section 9, Fraud Act 2006), false statements by company directors (section 19, Theft Act 1968), false accounting (section 17, Theft Act 1968), fraudulent trading (section 993, Companies Act 2006), and cheating the public revenue (common law).

[4] Hansard, HC Deb (13 September 2023), vol. 737, col. 938.

National Law Review, Volumess XIII, Number 324

Source URL:https://www.natlawreview.com/article/why-corporates-are-now-more-likely-face-criminal-

prosecution-actions-their