Browne Jacobson

Failure to prevent fraud: how can my organisation prepare?

22 November 2023

As its title suggests, the Economic Crime and Corporate Transparency Act (the **Act**), which received Royal Assent on 26 October 2023, sets onerous standards on UK corporates in the fight against financial crime.

A new strict liability offence of "failure to prevent fraud" makes large companies and partnerships (as defined below) liable for fraud committed by employees and associates.

The Offence

The failure to prevent offence applies to large organisations that meet two of the three following criteria: more than 250 employees; a turnover of more than £36 million; and/or assets of more than £18 million (**organisation(s)**).

Following the model established by the Bribery Act 2010 and replicated in the Criminal Finances Act 2017 in respect of tax evasion, the offence of failure to prevent fraud is committed if an "associate" (such as an employee, agent or person performing services for or on behalf of the organisation) commits a specified fraud offence with the intention of benefitting the organisation or its customers/clients.

The fraud offences include false accounting, fraudulent trading and cheating the public revenue. A guilty organisation is liable to an unlimited fine.

Defence of "reasonable procedures"

An organisation that can show it had "reasonable procedures" in place to prevent the fraud, or that it was not reasonable to have such procedures in place, will have a defence.

The government must publish guidance on what reasonable procedures look like before the new offence becomes law, but it could be several months until this guidance is available. Organisations looking to get ahead of the curve will find it useful to look at guidance provided in similar scenarios in the interim.

Failure to prevent bribery

The failure to prevent bribery offence under section 7 of the Bribery Act 2010 marked a revolutionary elevation in corporate criminal liability. Using slightly different language, an organisation seeking a defence to the section 7 offence must establish (on the balance of probabilities) that it had established "adequate procedures" to prevent bribery. The Ministry of Justice has issued separate guidance on measures that are likely to be considered adequate.

The guidance sets out six key principles and the criteria that investigating and prosecuting bodies will use to evaluate them. They include: proportionality; top-down commitment from senior management; risk assessment; communication (including staff training); and monitoring and review.

Importantly, the Crown Prosecution Service has acknowledged that there is a distinction to be drawn between the actions of a rogue agent or employee despite robust corporate procedures, and a wholesale failure to put risk management measures in place. It is hoped

that future guidance under the Act will take account of these nuances. The shift of language from “adequate” (in the Bribery Act 2010) to “reasonable” procedures suggests that the threshold for a defence may be more attainable under the Act.

Reasonable steps and the Equality Act

Equality laws have long provided for a “reasonable steps” defence, under which organisations will not be liable for acts of discrimination committed by their employees provided they can demonstrate that they took all reasonable steps to prevent the conduct from occurring.

In practice, whilst a policy and training are a good place to start, much more is expected. Organisations must ensure that the policy and its ethos is embedded into the organisation and its culture. This includes ensuring that polices are regularly reviewed and updated and are consistent with current guidance and best practice. Equally, the requirements of the policy need to be communicated to individuals in the organisation so that they are clear on what is expected of them and the consequences of any breach. In this respect, training should be reviewed and refreshed at appropriate intervals.

Of course, a policy and training have little impact if the ethos of this is disregarded in the day-to-day operation of the organisation. Therefore, those in a position of responsibility are expected to lead by example and model the behaviours they expect of their staff. Equally, when concerns are raised, they should be taken seriously, investigated and appropriate action taken where any concerns are well founded. By taking these steps it should create a culture of openness and accountability. As is considered below, wider considerations on diversity, equity and inclusion are all likely to have an impact in this regard.

The impact of gender diversity on risk

Recent analysis has established a direct correlation between higher numbers of female board members and a decreased risk of fraud. Whilst organisations may simply be drawing from a wider talent pool, separate research also suggests that diversity itself brings a natural and healthy level of conflict, reducing the risk of “groupthink”. There is, of course, a balance to be struck between an appropriate level of constructive challenge and harmful disruption. It is, however, not hard to see increasing diversity – whether gender or otherwise – as a positive step to increase representation. Where different views and perspectives are welcomed and encouraged, dissenting voices are more likely to be heard and considered.

Containing insights and trends from the 2023 reporting season, Thomson Reuters’ recently published *“Annual reporting and AGMS 2023: What's Market practice?”* report suggests that board diversity is still some way off. As of 13 October 2023, just 65 FTSE 100 companies have achieved 40% or more female representation on their boards. Only 76 companies (40 FTSE 100 and 36 FTSE 250) have met the Listing Rule target of 40% female representation on the board, at least one woman in a senior position and at least one director from an ethnically diverse background.

As well as improving board level diversity, encouraging a move towards a safe and accountable environment through whistleblowing and complaints is hugely important for reducing the risk of fraud. Where staff feel able to raise issues without a fear of repercussion, risks can be detected early and escalated appropriately.

How do I prepare?

Organisations can begin to prepare now by thinking about the following:

- **Risk assessment** – where are your biggest corporate risks around fraud? What safeguards are required to address those risks? Does more need to be done?
- **Policies** - do you have existing policies aimed at preventing fraud? Are they robust enough or do they need an update? How do they link to other policies (such as whistleblowing and disciplinary procedures) and contracts of employment or service agreements?
- **Training** - does your existing training cover prevention of fraud, behaviours expected of staff, how they should report any issues of concern and how they will be supported?
- **Awareness** - how do you keep your policy and training alive in the workplace so that it becomes part of the culture? Are the organisation’s behavioural standards linked to individuals’ performance/objectives? If not, should this be considered further, especially in respect of managers/leaders?
- **Accountability** – are concerns adequately dealt with and documented? Are there any areas of weakness? Are any internal procedures vulnerable to failure, and if so, what is the learning from this? Who will be the “gatekeeper” responsible for ensuring that the necessary review happens?

- **Diversity review** - how diverse is the make-up of the board/organisation? Does this pose any risks from an accountability perspective? What steps could be taken to improve diversity?

Once a thorough audit has taken place, organisations should implement their plans to plug any gaps. It would be prudent to document any decision-making process regarding the steps and procedures put in place including any reasons for omissions. This means that procedures can be revisited in a targeted way once Government guidance is published.

Further changes on the horizon

Through reforms to the “identification principle”, the Act makes further changes to the way that criminal liability for economic crimes more generally can be attributed to a company through the conduct of “senior managers”.

Previously, criminal liability for individual acts could only be attributed to a company when committed by a person who was its’ “directing mind and will”. Organisations with complex management structures within which responsibility was fragmented across large organisations, often across multiple jurisdictions, created difficulties for prosecutors seeking to meet this threshold. The Act widens the range of employees who can trigger corporate criminal liability, making it easier to prosecute businesses for economic crimes.

In the coming weeks we will be releasing a further piece on the implications of this change, with practical recommendations.

With thanks to our authors for their contributions: Claire Rosney, Emma Grant, Sarah Hooton, Helen Simm and Olivia Dwan.

If you’d like to discuss the points raised further or need assistance with preparing for the new legislation, then please contact our team.

Key contact

Helen Simm

Partner

Helen.Simm@brownejacobson.com

+44 (0)330 045 2652

Related expertise

Services

Business crime and fraud

Corporate

Coverage disputes and policy interpretation

Employment services for healthcare

Financial crime