Can understanding insider risk help to prevent fraud?

by Anoushka Warlow and Tom McNeill of BCL Solicitors LLP, and Sarah Keeling, Julia Arbery and Lucy Cryan of StoneTurn

Introduction

Fraud has reached endemic levels in the UK and is now considered a threat to national security. As well as damaging the UK's reputation as a business centre, rising levels of fraud are impacting the private sector's bottom line and its commercial stability. The Association of Certified Fraud Examiners estimates total global losses due to fraud to be nearly US$5 trillion. Of this sum, fraud committed by an executive or employee (occupational fraud) accounts for approximately 40% of the total, equivalent to US$2 trillion.

The UK government is moving towards introducing a new corporate criminal offence: Failure to Prevent Fraud and Money Laundering. As currently drafted, the offence would hold commercial organisations criminally liable for fraud or money laundering offences committed by associated persons where the organisation does not have in place reasonable procedures to prevent such offences.

The draft offence, currently contained within the Economic Crime and Corporate Transparency Bill, is working its way through the legislative process and has been the subject of much debate. It is not yet in its final form, but the bill is expected to receive Royal Assent this year. We expect guidance to be issued and the offence to come into force in 2024, but commercial organisations would be wise to start thinking now about their fraud prevention procedures.

Failure to Prevent Fraud and Money Laundering— an overview

As it currently stands, the Failure to Prevent Fraud and Money Laundering offence will be made out where:

1. An **'associated person'** of a **'relevant body'** commits a relevant **'fraud or money laundering offence'**; and
2. The relevant fraud or money laundering offence is **intended to benefit** (whether directly or indirectly)
   - **a.** the relevant body, or
   - **b.** any person to whom, or to whose subsidiary, the associate provides services on behalf of the relevant body.

StoneTurn

The relevant body is not guilty of an offence where the relevant conduct was **intended to harm** the body.

It is a defence for the relevant body to prove that it had in place such **prevention procedures** as it was reasonable in all the circumstances to expect.

Where a commercial organisation is convicted, unlimited fines can follow.

Breaking that down:

What is a 'relevant body'?

For the purpose of the Failing to Prevent Fraud and Money Laundering offence, a 'relevant body' is a UK company or partnership which carries out business in the UK or elsewhere, or a company or partnership wherever it is formed which conducts business in the UK.

Who is an 'associated person'?

An associated person is an employee, agent or subsidiary, or someone otherwise performing services for or on behalf of the relevant body.

What is a 'fraud or money laundering offence'?

As currently drafted, the relevant fraud offences are: fraud by false representation, fraud by failing to disclose information, fraud by abuse of position, obtaining services dishonestly, participation in a fraudulent business, false accounting, false statements by company directors, fraudulent trading, and cheating the public revenue.

As it currently stands, a relevant money laundering offence means an offence under the Proceeds of Crime Act 2002 of concealing etc. (section 327), arrangements (section 328).

However, it is possible that the list of relevant fraud or money laundering offences may be subject to change, either before the legislation comes into effect, or at some point afterwards, by way of amendment.

Intended to benefit the relevant body?

The associated person who commits the relevant fraud or money laundering offence must intend (directly or indirectly) that offence to benefit the relevant body, or benefit any person to whom the associate provides services on its behalf. No offence will be committed where the offence was intended to harm the commercial organisation.

The offence may be made out where, for example, the associated person intends primarily to act for their own benefit, but where that benefit is also felt by the commercial organisation (for example, an employee who fraudulently over-bills a client in order to boost their own performance figures, but also company revenue).

Reasonable fraud prevention procedures

Requiring commercial organisations to prevent fraud imposes a considerable burden. While the offence requires only that the prevention procedures be 'reasonable', what will be 'reasonable' in the context of each individual organisation is difficult to anticipate; and a procedure is much less likely to be judged as reasonable where it did not in fact prevent the offending.

The Bill as currently drafted envisages that the Secretary of State will be required to publish guidance on the procedures which could be put in place, however, it is likely that any guidance will be relatively high-level and principle-based. Given the wide scope of the offence, and the fact that it will cover a very broad range of sectors with very different risk profiles, it is unlikely that any published guidance will provide a clear framework for what an organisation should reasonably do to prevent fraud.

Moreover, very little guidance exists from other 'failure to prevent' offences. The Failure to Prevent Fraud and Money Laundering offence is modelled

on the existing offences of failing to prevent bribery (introduced via the Bribery Act 2010) and failing to prevent the facilitation of tax evasion (introduced via the Criminal Finances Act 2017). However, despite existing on our statute books for some years, neither of those offences has produced any meaningful judge-led guidance on how the 'reasonable procedures' defences work in practice or how they will be interpreted in contested criminal proceedings.

It will, therefore, be largely down to commercial organisations and their advisors to assess the types of controls required, by reference to organisation-specific factors, and to put in place bespoke fraud prevention procedures sufficient to meet the requirements of the new offence.

Reasonable money laundering prevention procedures

Anti-money laundering procedures are already well established for organisations operating in the regulated sector and for many organisations which are not. It remains unclear how the new offence would interface with the existing regime.

Where does Insider Risk fit in?

Organisations should start to consider now whether existing fraud risk assessments, policies, systems and controls adequately address the risk of not only outward but also inward fraud. Do they explicitly reference fraud committed on behalf of the organisation and by 'insiders'?

An insider can be considered as anyone to whom you have granted authorised access who then uses, or intends to use, that access for unauthorised purposes. An 'insider' can be anyone (an employee, a contractor, a business partner, or someone in the supply chain) who is trusted with physical or virtual access to a firm's assets and who can therefore cause harm.

Effective Insider Risk programs seeking to prevent and detect harm caused by insiders should:

- Assess and regularly update the evolving insider risk for the organisation.
- Develop a "response plan" to an insider incident: including how to respond, how to minimise damage and retain stakeholder trust.
- Ensure consistency and clear lines of responsibility for the management of Insider Risk.
- Understand and pay close attention to red flags: (for example, an individual's behaviour, performance or financial habits; absenteeism).
- Nominate a C-Suite and Board member who is accountable for Insider Risk.
- Execute spot audits.
- Put in place clear and proportionate policies and procedures.
- Implement ethics and compliance training.
- Ensure robust speak up procedures, a strong 'tone from the top' and a focus on culture.

If Insider Risk programs exist, they are often designed to prevent and detect misconduct targeted at an organisation, whether that be fraud, data loss, theft, sabotage, or the leaking of sensitive information.

However, an Insider Risk program can also act as an effective tool to identify and mitigate the risk posed by associated persons who might act dishonestly in the misplaced belief that they are acting in the best interests of the organisation.

Companies who are looking to refresh or update existing risk management processes in anticipation of the introduction of the new offence would benefit from looking closely at the controls they currently have in place to prevent, detect and mitigate insider

fraud. They also need to consider now how any existing programme can be adapted to prevent and detect any broader risks of misconduct committed in the interests of a company.

With the introduction of the new offence, organisations will also need to consider how employees or other potential insiders might rationalise committing fraud "on behalf" of their organisations. Are employees under pressure to meet targets, win contracts, or achieve unrealistic levels of performance? Has the firm been recently re-structured or involved in M&As (changes which promote uncertainty and increase the likelihood of insider risk)? Could misplaced loyalty lead an insider to obtain services dishonestly, make false representations or otherwise commit fraud that they believe will benefit their employer?

What actions should organisations take now

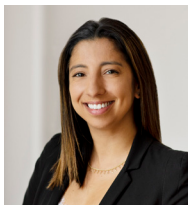
From an Insider Risk perspective, some practical measures that organisations can consider now include:

- Ensure that training, communication and 'tone from the top' attribute the same level of importance to preventing all types of fraud ("inward" and "outward"). Visible and clear policies, standards and procedures relating to fraud should be communicated consistently and regularly across the organisation.
- Remind employees that outward fraud should be escalated and reported using the same mechanisms (including whistleblowing channels) as inward fraud. Now is a good time to assess your 'speak up' programme. How, and with what frequency, does your organisation measure the effectiveness of its whistleblowing programme? Are your leaders committed to promoting a culture of speaking up?
- Conduct an updated insider risk assessment to take account of any evolving internal and external risk factors. For example, the pandemic and the rise of remote working has increased the risk of insider fraud, given the higher number of employees who are isolated and have infrequent interactions with co-workers and supervisors.
- Develop "response guidance" to an insider incident covering how to respond, minimise damage and retain stakeholder trust. Ensure that this response guide considers all types of insider act and includes outward as well as inward fraud.
- Conduct enhanced due diligence on any employees or service providers (including third party agents) who have access to the firms' most sensitive data or assets.
- Ensure that regular monitoring and reviews of fraud systems and controls (to set up 'trip wires' and to spot 'red flags') are in place, and that reviews consider changes in the risk profile of the business. Monitoring and reviews may be conducted internally or through an independent external party.

Conclusion

Tackling fraud and money laundering is hard: fraudsters are agile, adaptive, inventive and fuelled by the evolution of technology. The geopolitical risk landscape is also challenging, and complex risks are continuously emerging and evolving. Organisations need therefore to be adaptive, agile, inventive and holistic in their approach to detecting, preventing and mitigating all types of offending. The new Failure to Prevent Fraud and Money Laundering Offence is another incentive to revisit existing risk management programmes, including those that cover Insider Risk. A timely review and remediation of these programmes may well be one of the best ways to protect your organisation.

About the Authors



Anoushka Warlow, is a Partner at BCL *specialising in acting for individuals and companies in relation to all aspects of financial crime, principally cases involving complex allegations of fraud, bribery and corruption. Anoushka's expertise includes acting in foreign and cross-border investigations, defending individuals in private prosecutions, and advising on civil fraud matters.*

Tom McNeill, is a Partner at BCL *specialising in regulatory/corporate crime and financial crime. His expertise includes corporate and individual manslaughter, health and safety (including coroner's inquests), environmental protection, firesafety, all types of fraud, bribery, and money laundering.*

Sarah Keeling, a StoneTurn Board Member and Partner, *with over 30 years of experience as a senior British government official and trusted advisor, specialises in global investigations and geopolitical risk. Her expertise supports corporate Boards, family offices, PE firms and alternative asset funds, advising on holistic strategies to navigate operational, reputational, investment, and security challenges.*

Julia Arbery, a Partner at StoneTurn, *has more than 15 years' experience assisting multinational corporations with the development and implementation of effective ethics and compliance programs across their global operations. Notably, Julia aided the DOJ-appointed Independent Compliance Monitor for Volkswagen AG— one of the largest and most high-profile corporate compliance monitorships in history.*

Lucy Cryan, a Manager with StoneTurn, *has a background in forensic accounting investigations, and dispute resolution. Over the course of her career, Lucy has conducted investigations into fraudulent activity, accounting errors, professional negligence and bribery and corruption.*