Corporate Crime and Investigations 11th Annual Conference: Corporate Fraud

9 July 2024

From preparation to judicial approach, we summarise the major talking points from the event

On 20 June 2024, the eleventh annual Corporate Crime and Investigations Conference was held in London. We have set out below a summary of the highlights from the event. Please feel free to get in touch with one of the listed contacts if you would like to discuss any of these issues further.

The Conference centred on "Corporate fraud – navigating the changing landscape", with panel sessions on: "fraud liability and risk mitigation", and "fraud response and recovery".

Fraud liability and risk mitigation

The Economic Crime and Corporate Transparency Act 2023 ('ECCTA') received royal assent in October 2023. One of the reforms introduced by this act is the failure to prevent fraud offence ('FTP offence'), which is expected to come into force in 2025. Further detail on the FTP offence can be found in our previous briefing and our ongoing podcast series.

Following a refresher on the changes being introduced by the ECCTA, the panel discussed some of the trickier legal areas that may arise in applying the FTP offence and the separate reforms to the identification doctrine, including the SFO's views on some of those issues and its current priorities in relation to the investigation and prosecution of fraud. We have highlighted some of the key topics in the following paragraphs.

Preparation

The audience were asked how prepared their companies were for the FTP offence, in particular, in relation to the development of "reasonable fraud prevention procedures", which will act as a defence to the FTP offence. In that poll, 42% voted that they had done nothing substantial to prepare for the offence and they were waiting for guidance. 14% of the audience had completed the risk assessment and any policy/procedure enhancements, with plans to top-up once the official guidance is published.

It appears that many companies are therefore waiting for the official guidance on what constitutes reasonable fraud prevention procedures (which is anticipated to be relatively similar to the other guidance already in force in respect of the offences of failure to prevent bribery and failure to prevent the facilitation of tax evasion). It was expected that guidance would not be released by the Ministry of Justice until after the election, and there will be at least six months between the guidance and the offence coming into force.

Jurisdictional approach

As discussed in more detail in our blogpost, the jurisdictional scope of the FTP offence is pinned to the jurisdiction of the underlying fraud offence; to be in scope of the offence the fraud has to have a UK nexus. This can include, for example, fraud by an overseas fraudster which targets UK victims.

The audience were asked how they are approaching the jurisdictional reach of the FTP offence within their preparations; 53% of those polled were carrying out a group wide project (ie, approaching their fraud prevention procedures on a jurisdiction-agnostic basis), and 35% were focusing on the UK initially, with a view to expanding globally as a second stage of the project.

Significant areas for uplifts/enhancements

When asked what are going to be the most likely significant areas for uplifts/enhancements to address the offence, 34% of the audience voted for training, and 21% voted for associated person controls.

Fraud response and recovery

The second panel session focused on a scenario, involving a company who may have been a victim of fraud, resulting in the loss of significant funds. The audience was asked to put themselves in the position of the General Counsel of the company, and rank their concerns/areas of focus by order of priority.

The number one priority was to secure the company's systems and understand the extent of the breach. Recovering the company's money placed third, behind identifying and deterring complicity by employees as the number two priority. The fourth and fifth priorities were to deter fraudsters external to the company, and support law enforcement agencies in punishing wrongdoers. We have set out below some key takeaways from the discussion of these priorities.

Determine the extent of the breach and secure systems

Cyber expert, Peter Dalton, discussed efforts to find the root cause of the fraudulent activity, which would require a combined effort between internal Legal and IT teams, and any external forensic experts instructed. If it is determined that the system has been compromised, the teams should work to assess how this has occurred and how wide the breach is, eg, to determine if personal data has also been stolen, which would lead to considerations of notifications. If the fraudsters still have access to the system, an immediate step would be to sever any connection.

Details on the firm's cyber risk capabilities can be found here.

Identify and deter complicity

Time on the day prevented a detailed consideration on how to conduct an investigation to identify any complicit employees – as this could be a panel in itself. However, our criminal investigations team identified three top priorities to keep in mind:

- preservation of evidence, to ensure that no relevant information is disposed of;
- scoping the investigation, to figure out what the aims are and work with regulators and law enforcement; and
- identifying individuals who will conduct the investigation – ensuring that the investigation team are not involved in any of the alleged misconduct. The team will often report to a sub-committee from the board.

Recover the company's money

Heather Rankin, a civil fraud expert, explained that an early step should be to notify the victim's paying bank, which may be able to prevent the money from being transferred onward. The receiving bank should also be notified, as it may take steps to freeze the account due to its own money laundering obligations. Kyle Wombolt, Head of our global practice and based in Asia, spoke about the approach of international receiving banks in Hong Kong and Singapore.

Civil actions

Heather discussed potential civil actions, including a freezing order (domestic or worldwide) to prevent the respondent bank from dealing with, disposing of, or diminishing the value of the assets.

She also spoke about Bankers Trust/Norwich Pharmacal orders against the banks into which stolen funds have been paid. This order requires the third-party bank to disclose information about the movement of the funds to the victim, helping the victim pursue legal redress.

She cautioned as to the likelihood of substantial costs being incurred, and the need for a corporate victim to weigh the amount of loss against the time and cost of pursuing civil action to chase that loss.

Criminal actions

Our corporate criminal team spoke about the powers of the criminal authorities, including to seek a pre-charge restraint order and subsequent order for disgorgement, which could allow the assets to be returned.
As explained by the panellists, whilst it is possible to recover lost funds by working with criminal law enforcement, there are two common barriers to recovery:

- the high burden of proof in a criminal case; and
- the fact that victims are not in control of the investigation and are reliant on public enforcement agencies who are often operating with limited resources.

In circumstances where a public prosecution may not be pursued, perhaps due to public resource constraints, there is also the option to bring a private prosecution. This can allow a greater measure of control for the victim, although it comes with significant time and cost challenges.

Other claims

The panellists touched on other potential claims, such as against IT providers for failing to have adequate security, or the banks for not exercising reasonable care.