The UK's fraud landscape in 2023

Practical Tips to Support your Business

The scale of fraud in England and Wales continues to rapidly increase, making up an alarming 41% of all crime against individuals. 2022 saw numerous reports published which all broadly conveyed the same message: fraud is a huge financial, social and political problem for the UK.

There is some promising news, following a lengthy inquiry, on 12 November 2022 the House of Lords and Digital Fraud Committee published its report 'Fighting Fraud: Breaking the Chain'. The report made various recommendations including a new cabinet-level subcommittee to tackle fraud and a new corporate criminal offence of a failure to prevent fraud.

For further insights on the current fraud landscape and a deep dive into the House of Lords Report's recommendations and potential impact, read our analysis here.

Even if and when firmer policies are in place and greater resources are allocated to combat fraud, the need for internal fraud prevention remains as important as ever.

In our experience, the simplest solutions can often prevent fraud. By way of example, we have set out a few practical tips for your business in order to protect against the following risks:

1. Human error

Human error will always be one of the key vulnerabilities of an organisation's infrastructure. In particular, one of the key features that may make a person more likely to become a victim of fraud is digital exclusion – as it is thought that over a third of the UK's workforce are thought to lack the technological skills needed for safe online behaviour. Providing detailed IT training, raising awareness of internal policies and procedures and engaging with trusted suppliers to carry out incident simulation are all crucial parts of fraud prevention.

2. Weak links in the supply chain

A business is only as strong as its weakest link – which goes for its supply chain too. When is the last time you ran through the contracts you have with your supply chain? Ensuring proper provisions are in place within your external supplier contracts will help provide protection for your business such as requiring system back-ups, a high standard of data protection compliance and rights to audit.

3. Long-standing areas of vulnerability

More often than not when clients come to us following the discovery of an incident, such as siphoned-off monies or VAT fraud, when sharing the findings of our investigations, we hear that the weak-spots in the

systems were not unknown and had been on the 'fix list' for some time. Working with teams across the business to identify the risks your business is most prone to and ensuring that the elimination of weak-spots is prioritised helps reduce the risk of penetration.

4. Response time and process

Does your business have a response plan in place which clearly sets out who is responsible for leading and co-ordinating the business response should an incident be uncovered? This will include considering whether to contact the police or Action Fraud, whether to inform your insurers, which legal and professional advisors will assist, and what communication must go to employees, stakeholders and the media. Lack of a response plan could create further disruption and affect business continuity.

Our Commercial Litigation team specialise in fraud and cybercrime investigations as well as whistleblowing. If you would like to find out more about how we can support your organisation in reacting to or preventing instances of fraud, please contact Jamie De Souza, Elizabeth Mulley or Amy-Rose Warman for a confidential discussion.

Key contacts

Jamie De Souza
Partner, Dispute Resolution and Litigation
+44 (0)121 214 8847
JDeSouza@trowers.com

Elizabeth Mulley
Senior Associate, Dispute Resolution and Litigation
+44 (0)121 214 8864
EMulley@trowers.com

Amy-Rose Warman
Associate, Dispute Resolution and Litigation
+44 (0)121 203 5672
AWarman@trowers.com