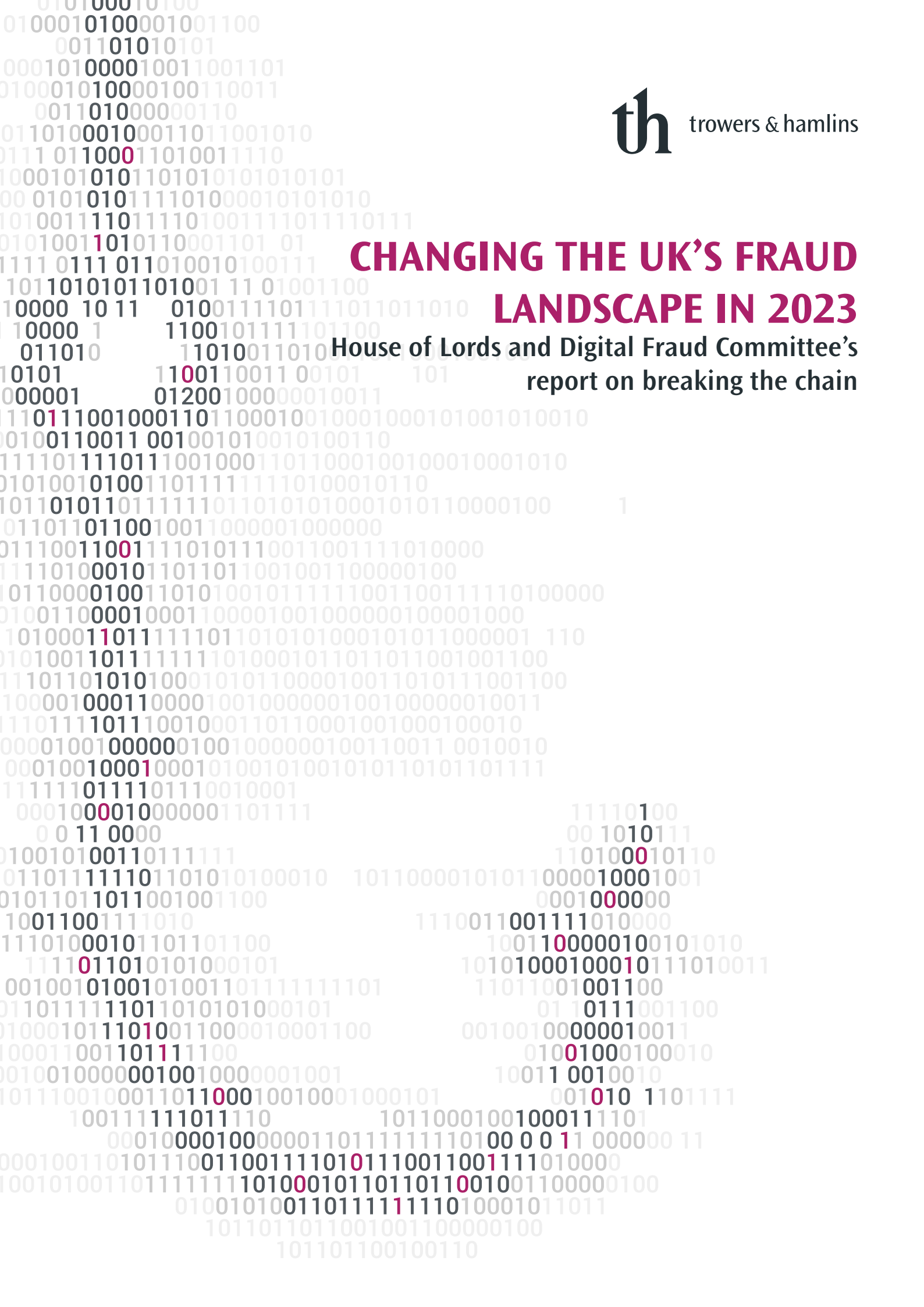

trowers & hamlins

# CHANGING THE UK'S FRAUD LANDSCAPE IN 2023

## House of Lords and Digital Fraud Committee's report on breaking the chain

# Contents



Follow us and join our online discussion

– Trowers & Hamlins – @trowers – @trowers_law

# UK fraud landscape - In context

The scale of fraud in England and Wales continues to rapidly increase, making up an alarming 41% of all crime against individuals. These figures are only set to increase, with Commander Nik Adams, Economic Crime Portfolio lead at the City of London Police, predicting between a **25% – 65% growth in fraud over the next four to five years.**

2022 saw numerous reports published which all broadly conveyed the same message: fraud is a huge financial, social and political problem for the UK. UK Finance's Annual Fraud Report went as far as to say that there is an epidemic of fraud in the UK (the "UK Finance Report"). This is hardly surprising following the pandemic years of 2020 and 2021, in which fraudsters quickly adapted to exploit our isolation and increased dependence on cyberspace.

**2014%**
to £9.5 billion in 2021

BDO's FraudTrack explores recent trends in fraud each year, with the 2022 key findings ("FraudTrack") illustrating that the monetary cost of fraud in 2021 was more than ever; rising by 2014% to £9.5 billion due principally to fraud conducted on government support schemes. This, of course, only takes into account reported fraud which has undoubtedly been affected by court closures and backlogs from COVID-19. PwC's Economic Crime and Fraud Survey notes the highest level in its 20 years of research of its surveyed organisations experiencing fraud within the past 24 months (at 52%) (the "PwC Survey"). Taking into account these concerning findings, it is now critical that the executive, legislature and judiciary push fraud to the forefront of the agenda.

## Breaking the chain

There is some promising news that, following a lengthy inquiry, on 12 November 2022 the House of Lords ("HoL") and Digital Fraud Committee published its report 'Fighting Fraud: Breaking the Chain' (the "HoL Report"). As commented upon, the HoL Report discusses the problem that is costing the economy billions every year[1] in the context of an increasingly digital world and a disturbing upsurge in authorised push payment ("APP") fraud. Recommendations include imposing delays to high-risk payments, a new cabinet-level subcommittee to tackle fraud and a new corporate criminal offence of a failure to prevent fraud.

It is clear that radical changes are needed to properly deal with the UK's fraud crisis, and whilst the HoL Report goes some way to address this, more is needed by way of collaborative action (as addressed in the UK Finance Report) and to make the digital platforms we use safer (as set out in the PwC Survey).

This report analyses the key recommendations in the HoL Report, what we would like to see in 2023 and our practical tips to protect your business against common fraud risks.

1 - Latest data shows losses over the past year total £4billion – ONS 'Crime in England and Wales: Appendix tables' (27 October 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2022#fraud

# Problems with the current landscape


Although individuals are at higher risk of being targeted by fraudsters, businesses have also been severely impacted. In the first half of 2022, it is estimated that over 40 million UK adults were targeted by fraudsters, with a loss of £609.8 million to all types of fraud[2]. The PwC Survey explains that in relation to companies, of those with more than US$10bn in revenue **52% reported experiencing fraud within the past 24 months**, with those at less than US$100m in revenues reporting slightly lower at 38%. Of those 38%, 22% of them suffered a financial impact of US$1m or more from collective fraud incidents.

APP fraud, being when a person or business is tricked into sending money to a scammer posing as a legitimate payee, was the most prevalent costing £249.1 million, followed by impersonation scams (£90.5 million) and investment scams (£61.2 million).

The HoL Report found that:

- Law enforcement agencies are under-resourced and underfunded for the fight against fraud, with only 1% of law enforcement focussing on economic crime[3]. It is clear that this is nowhere near sufficient to counter the fraud figures of 41% of all crime as mentioned above. The government has promised to add 20,000 officers to the force by March 2023[4]. As at 31 December 2022, 16,753 additional police officers have been recruited directly from the Police Uplift Programme, with a further 472 additional officers recruited through other funding streams[5]. There still, however, remains a serious shortage of experienced detectives and digital forensic specialists, which the promise of additional officers will not address[6].
- There are too many bodies involved with a responsibility for counter-fraud policy which has led to a lack of accountability and inefficient policymaking.
- Organisations making up the fraud chain are not uniformly incentivised and that a collective effort of private and public sectors needs to be achieved to ensure vigilance and prevention. The jointly published Home Office and UK Finance Economic Crime Plan 2019 to 2022 sets out how to better harness the combined capabilities of the public and private sectors to make the UK a leader in the global fight against economic crime ("UK Finance Report"), however, there has been little progress regarding a performance framework to monitor progress towards its objectives (with 40% having been achieved in February 2022). The plan has also not been updated since 4 May 2021, despite the April 2022 report detailing the 52 actions contained in the plan.

---

2 - Citizen's Advice 'Over 40 million targeted by scammers as the cost-of-living crisis bites' (12 June 2022): https://www.citizensadvice.org.uk/about-us/about-us1/media/press-releases/over-40-million-targeted-by-scammers-as-the-cost-of-living-crisis-bites/
3 - Oral evidence taken before the Treasury Committee on 25 January 2021 (Session 2019–21), Q 2 (Graeme Biggar) and Q 222 (Andy Cooke)
4 - Home Office (31 March 2022) National Statistics: Police workforce, England and Wales (updated 27 July 2022)
5 - Home Office (27 July 2022) Official Statistics: Police officer uplift, England and Wales, quarterly update to 31 December 2022 (updated 27 January 2023)
6 - Criminal Justice Joint Inspection (May 2022), The impact of the Covid-19 pandemic on the criminal justice system- a progress report

- The UK's AML/CTF regime is not stringent enough and will undergo a much-needed targeted review in 2023.The telecommunications sector, by way of example, has been allowed to stand by while fraud is facilitated via its services for too long. In fact, perhaps surprisingly, cybercrime is consistently one of the biggest threats to industries, amounting to 50% of the fraud experienced by the technology, media and telecommunications sector (PwC Survey). In addition, Ofcom has not applied sufficient pressure to this sector to ensure scam reporting services as transparent to encourage user reporting.
- There is a significant link between fraud and technology. This topic was debated on 6 December 2022 by the Midlands Fraud Forum who hosted a discussion on "does modern technology help facilitate or fight fraud?" in which Helen Briant, a Partner at Trowers & Hamlins, was a panellist and gave her views that it more often than not tends to be a facilitator as opposed to a method to fight fraud. The HoL Report notes that a range of long and shorter-term factors have enabled the UK to become a centre for digital fraud – globalisation, digitalisation of features such as online banking, and shorter-term factors like COVID-19, the cost-of-living crisis and the emergence of cryptoassets all play a role in the UK's rise in fraud. In 2021 80% of fraud was cyber-enabled. The HoL Report notes several of the cyber-enabled fraud offences that appear increasingly common such as romance fraud via online dating apps, cryptocurrency related scams such as confidence scams or support impersonators and online fraudulent advertising.

# Six steps to breaking the fraud chain

Against the above backdrop, the HoL appointed the Digital Fraud Committee in January 2022. The Committee received individual submissions and heard evidence from 45 oral witnesses from a range of stakeholders including academics, victims and law enforcement representatives in producing the HoL Report. The Midlands Fraud Forum hosted a roundtable in 2022 for the Select Committee, at which members of Trowers & Hamlins were invited to attend and provide their views.

The HoL Report set out its views on six steps to breaking the fraud chain:

1. For the speed of payments to be delayed in certain circumstances to allow banks sufficient time to review risk signals and contact the customer if necessary. As such, the Payment Systems Regulator must consult on putting in place measures to achieve this.
2. That a new corporate criminal offence of a failure to prevent fraud must be introduced across all sectors, accompanied by substantial financial penalties. This would replicate failure to prevent offences in existing law such as bribery and tax evasion.
3. Fraud should be included within the Strategic Policing Requirement ("SPR"). The SPR sets out the Home Secretary's assessment of the national threats that police must prioritise in England and Wales.
4. A cabinet subcommittee should therefore be established made up of Secretaries of State which is chaired by and accountable to the Security Minister.
5. The Online Safety Bill (the "OSB") is set to try and shake up the rules and regulations for firms that host user-generated content and search engines. The OSB is presently at Committee stage and due to move on to the Report stage thereafter.
6. That the Government oversees the introduction of a single, centrally-funded consumer awareness campaign in partnership with industry to create clear advice for consumers to follow to help prevent and report fraud.

# What's next following the recommendations?

So far as the HoL Report is concerned, the ball is now in the Government's court; it was due to respond to the Report's recommendations by mid-January 2023. It will be interesting to see how the Government responds to the recommendations in the HoL Report.

In our view, whilst it is welcome news to see positive steps are being made towards creating a more cohesive fraud prevention framework that has some teeth, it is unlikely that the Report's recommendations will be sufficient to slow down, let alone bring to a halt, the continued upsurge in fraud as set out in the UK Finance Report, FraudTrack and the PwC Survey to name a few.

Of the recommendations put forward, we consider the most well-received change will be the introduction of the offence of "failure to prevent fraud". The HoL Report emphasised that regulatory punishments may not be a sufficient deterrent and therefore suggest a failure to prevent fraud as a corporate criminal offence of strict liability (i.e. if a company fails to prevent fraud they are liable). Those who are involved in the fraud chain will need to ensure that they have in place measures to prevent employees and agents from committing fraud for the benefit of the company.

We note that there may be a defence available if companies can prove they had sufficient prevention procedures in place as was reasonable in the circumstances, or that it was reasonable to not have any procedures in place. If the Government agrees with the Report's proposal, companies will need to ensure strict policies and procedures are in place as well as undertaking thorough risk assessments and checks in order to avoid the risk of financial penalties as well as any potential commercial repercussions, such as adverse media attention and loss of business. Since its first reading in the HoL on 30 January 2023, the government has now indicated it would look at adding a "failure to prevent" fraud offence to the Economic Crime and Corporate Transparency Bill, however at present this may only apply to solicitors, accountants and casinos.

Although the Report also pushes for the OSB to be brought forward, we have concerns regarding the duty of care that would be imposed and how this would work in practice. Until now only user-generated scams were covered; the OSB will hold those who publish paid-for fraudulent adverts on their services accountable whether controlled by the platform itself or an advertising intermediary. However, the OSB will only apply to limited bodies in the advertising supply chain such as platforms and search engines; with the onus on social media firms to self-police and Ofcom to oversee whether companies have adequate measures in place. Social media companies see hundreds and thousands of advertising posts / videos every minute – it is not clear how this content can be censored effectively in practice beyond Ofcom publishing 'guidance' as a benchmark. Further, the UK is now on its fourth prime minister since the idea of legislating the digital world was first initiated, and as a result, copious inclusions have been made which has resulted in the OSB covering an impossibly broad range of topics – taking the edge off what could have been a sharp stick. In contrast to the "failure to prevent fraud" offence, our view is that it is unlikely the duty of care imposed in the OSB will be sufficient to tackle online fraud as was first envisaged.

# What would we like to see in 2023?

Whilst positive, it is clear that more will need to be actioned to break the fraud chain than the HoL Report's six steps. For example, other key themes that we consider are important, and have been identified in other reports, include:

- More effective collaboration between stakeholders involved, for example, regulators and legislators with the financial sector to ensure fraud prevention is an intrinsic part of systems (UK Finance Report). **It is clear that industries should be encouraged to collaborate and share data in order to reduce the risk of fraud,** however the Report does not make recommendations regarding the lack of incentive for companies / regulators to share data a part of its six steps. It is clear to us that a holistic approach is needed from everyone in the fraud chain and the sharing of data for the purpose of fraud prevention. We appreciate that data sharing is a very sensitive topic and must be addressed cautiously and with the correct legal guidance, however it is often the case that if companies in the fraud chain had talked about known risks then the fraud may have been prevented. Many companies live in fear that GDPR means data sharing within public and private sector companies will leave them at risk of receiving fines or legal action, which is often unfounded. For example, Article 6(1)(f) of the GDPR, the processing of data for the purposes of 'legitimate interests', is likely to be a safe harbour for companies in certain circumstances. Whilst there is no definition of legitimate interests, there is ICO guidance that sets out that fraud prevention and indicating possible criminal acts or threats to public security constitutes or should be regarded as a legitimate interest[7]. In addition, section 68 of the Serious Crime Act 2007 provides a power for a public authority to disclose information as a member of an anti-fraud organisation for the purpose of preventing fraud[8]. Examples of this working well include the UK Finance's Intelligence and Information Unit with 1.6 million compromised card numbers received through law enforcement and disseminated via the Unit to enable card issuers to implement the necessary precautions to protect customers.
- An overhaul of Companies House is desperately required to stop criminals hiding behind a corporate veil. Although there is some progress towards Companies House being provided with tools to fortify its systems pursuant to the Economic Crime Bill, it will need significant investment and assistance / regulatory powers in order to deter fraudsters. For example, currently businesses are expected to individually get in touch with Companies House to report a suspected case of fraud, which could be improved by implementing a seamless and efficient reporting process along with the risk of meaningful action to ensure fraudsters are penalised for their actions and other businesses / individuals are protected. These issues are explored further in our article Register or facilitator: Companies House criticised for insufficient measures to prevent business fraud.
- Whilst an awareness and consumer campaign will undoubtedly be helpful to ensure a single, co-ordinated approach to reporting and educate consumers, there is little messaging out there to deter those who are / have committed fraud in a pro-active approach. Particularly in light of the current economic climate and the predicted increase in fraud, the deterrence of criminals would be equally, if not more, important – for example in explaining the consequences of engaging in fraudulent activity.

7 - ICO, 'When can we rely on legitimate interests?': https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/
8 - Written evidence from Cifas (a not-for-profit membership organisation for fraud prevention): https://committees.parliament.uk/writtenevidence/107973/html/

- Each advancement of technology opens new doors for fraudsters to scam businesses and individuals, and it is likely that the UK law will never quite be able to keep up so that it is ahead of fraudsters. However, **the advancement of technology could be used more proactively as both a sword and a shield in combatting fraud.** We note that bank and card companies prevented £1.4 billion in authorised funds in 2021 (UK Finance Report), representing incidents that were detected and prevented equivalent to 65.3p in every £1 of attempted fraud stopped. Whilst there has been an increase in biometrics, AI and technology-assisted review for detecting fraud risks, its use and role in the fraud battle ought to be more widely utilised. For example, regular stress-testing of KYC procedures in order to address threats such as deepfake technology should be applicable beyond the financial sector and FCA review to cover all involved industries. Yet the HoL Report highlights that in any event the FCA has only taken action against 11 firms for inadequate AML, anti-bribery and corruption controls since 2018. This creates concern that there is still some way to go before regulators have sufficient clout and companies have the incentive to comply with KYC and AML requirements. To this end, it is promising news that the government has committed to spend £22billion on research and development to ensure it is at the heart of national security pursuant to the National Cyber Strategy 2022, which will hopefully affect online fraud prevention.

# Practical tips to combat fraud

The need for internal fraud prevention remains as important as ever; even when and if firmer policies are in place and greater resources are allocated to combat fraud.

In our experience, it can often be the simplest solutions that prevents fraud from occurring. 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[9]. 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.

9 - Lloyds Bank, UK Consumer Digital Index 2020 (2020), Appendix 44: https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/211109-lloyds-consumer-digital-index-2020-eds.pdf

Trowers & Hamlins works with its clients together with our trusted partners, such as cyber security companies and funders, in ensuring their businesses have assessed and accounted for the above risks as well as supporting them through the aftermath of when a fraudulent incident is discovered.

Please do not hesitate to contact the writers of this article should you have any queries on the implications of the Report on your organisation or want to know more about how we can help stress-test and improve your businesses' armoury.


**Jamie De Souza**
Partner
+44 (0)121 214 8847
jdesouza@trowers.com

**Helen Briant**
Partner
+44 (0)121 214 8867
hbriant@trowers.com

**Elizabeth Mulley**
Senior Associate
+44 (0)121 214 8864
emulley@trowers.com

**Hannah Jakeman**
Associate
+44 (0)121 214 8875
hjakeman@trowers.com

**Emily Sharples**
Associate
+44 (0)121 214 8874
esharples@trowers.com

**Meera Solanki**
Associate
+44 (0)121 203 5646
msolanki@trowers.com

**Amy-Rose Warman**
Associate
+44 (0)121 203 5672
awarman@trowers.com

**Rachel Storey**
Solicitor
+44 (0)121 203 5625
rstorey@trowers.com

trowers & hamlins

trowers.com