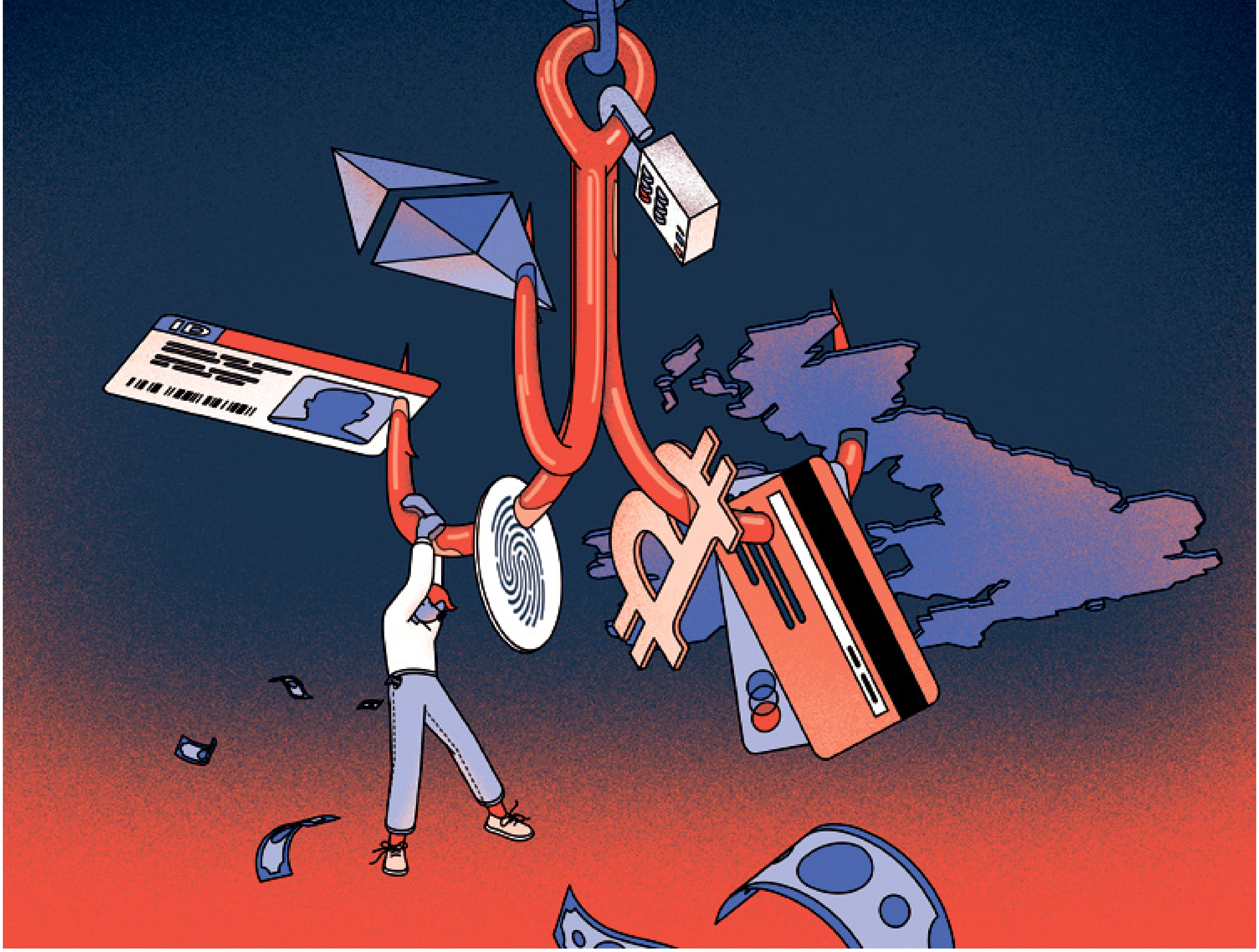
FRAUD & FINANCIAL CRIME



FRAUD & FINANCIAL CRIME

Distributed in THE TIMES

Published in association with O.R.X

Contributors

Fiona Bond
A freelance journalist covering all areas of finance and investing. She was formerly the commodities editor at *Interactive Investor*.

Laurie Clarke
A UK-based freelance journalist specialising in technology. Her work has been published in *The Observer* and the *New Statesman*.

James Gordon
A journalist and executive writer who has written extensively about business, technology, logistics, manufacturing and sport.

Sean Hargrave
A former *Sunday Times* innovation editor who works as a freelance journalist specialising in tech, financial services and digital marketing.

David Stirling
A freelance journalist who writes news and feature articles for national publications, including newspapers and business magazines.

Chris Stokel-Walker
A journalist and author who writes about technology and culture. He has had bylines in *The New York Times*, *The Guardian* and *Wired*.

Daniel Thomas
A writer and editor whose work has been published by outlets including *The Telegraph*, *Newsweek*, *Fund Strategy* and *EducationInvestor*.

Jonathan Weinberg
A freelance journalist and writer whose specialisms include technology, business and the future of work and society.

Raconteur

Campaign manager
Narinder Hayer

Reports editor
Ian Deering

Deputy reports editor
James Sutton

Editor
Sarah Vizard

Chief sub-editor
Neil Cole

Sub-editor
Christina Ryder

Commercial content editors
Laura Bithell
Brittany Golob
Joy Persaud

Associate commercial editor
Phoebe Borwell

Head of production
Justyna O'Connell

Design/production assistant
Louis Nassé

Design
Kellie Jerrard
Harry Lewis-Irlam
Colm McDermott
Sean Wyatt-Livesley

Illustration
Celina Lucey
Samuele Motta

Design director
Tim Whitlock

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3877 3800 or email info@raconteur.net
Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at raconteur.net

@raconteur raconteur-media @raconteur.stories

raconteur.net /fraud-financial-crime-2023

PREVENTION

Is your organisation ready for the downturn upsurge?

Fraud is widely expected to proliferate in the UK as a recession looms. A key challenge for businesses is to keep the criminals at bay without also repelling their customers

Daniel Thomas

Businesses are attractive targets for fraudsters at the best of times, but they're even more at risk during an economic downturn.

There are already signs that 2023 will be a damaging period in this respect in the UK. In November 2022, Cifas, a not-for-profit provider of fraud prevention services, reported that the number of cases of fraud committed by employees against their firms had risen by 25% year on year. It suggested that the ongoing cost-of-living crisis was a factor pushing more "staff members into committing dishonest conduct".

As trading conditions toughen, businesses tend to become more vulnerable to fraud, both internal and external. With their budgets shrinking, they may have fewer funds to devote to keeping their security processes up to date, for instance, while job cuts may leave them understaffed in key areas.

"Business owners who are under financial pressure may also become more susceptible to fraudsters promising monetary gain," notes Tina McKenzie, chair of UK policy and advocacy at the Federation of Small Businesses.

To protect themselves properly, companies must first understand the most prevalent forms of fraud so that they can train their staff to spot them, McKenzie advises. One of the most common is invoice fraud, where a criminal posing as a genuine supplier approaches a firm and asks it to change the details of the account it uses to pay them. In a similar vein, impersonation scams, where a fraudster contacts a company pretending to be a trusted organisation such as a bank or HMRC – or even a senior figure in the business – and convinces it to move money into another account.

There are several types of cyber fraud too, of course. They range from technologically sophisticated forms such as ransomware and distributed denial-of-service attacks to an enduringly popular group of techniques that rely more on social engineering to deceive their intended victims: phishing.

Luke Beeson is group CISO at Aviva and chair of the Chartered Institute of Information Security, a standards body that monitors online fraud threats. He reports that phishing remains the most common class of fraud committed against businesses, which puts the onus on employees to serve as the first line of defence against it.

"The risk of a successful phishing attack will be much lower if they understand why it's a threat, why they specifically might be targeted, what a phishing attempt looks like and what to do if they spot a suspicious email or link," he says.

They will therefore require comprehensive awareness training, says Beeston, but he adds: "The message won't sink in if you use too much cybersecurity jargon."

Many of the fundamental safeguards should already be familiar to all employees. For instance, no one should ever let themselves be convinced by an unsolicited caller to share sensitive data, download software or allow remote access to their computer.

"A good general rule to follow is: don't be rushed into doing anything," McKenzie says. "Fraudsters will often try inducing a sense of urgency, as people in a panic are more likely to act out of character and share information they would usually know to keep private."

Use strong passwords, which need to be changed regularly, she adds, and set up two-factor authentication for log-ins to important websites.

Any failure to uphold such basic defences is needlessly putting your business at risk. Yet firms must balance foiling fraud with maintaining a smooth customer experience, which isn't always straightforward, observes Caitlin Sinclair, head of payment solutions at the London Stock Exchange Group.

Online shoppers have become so used to interacting seamlessly with etailers such as Amazon that any company adding cumbersome security features to its website is likely to deter customers just as much as criminals, she warns.

"Consumers and SME users are increasingly basing their buying decisions on the process they have to navigate to make their purchases," Sinclair says. "Businesses must therefore prioritise the design of their onboarding and verification processes to remain relevant."

She adds that the security measures that firms adopt should vary according to their clientele. For instance, if you're a company that caters mainly to "digitally native" consumers who are happy to interact with you via a smartphone app, then adding an ID verification process that uses biometrics and open banking should do the job. If your target market is less comfortable using such tech (and perhaps includes extremely wealthy people), then a different approach that offers easy access to human support is likely to work better.

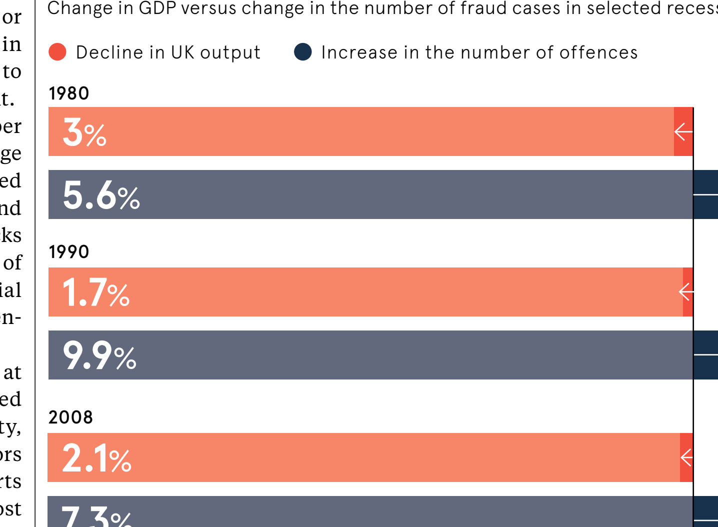
It's also important to remember that, although most cases of fraud against businesses are committed by outsiders, the threat of an inside job is very real – as the 2022 report from Cifas indicated. In cases of invoice fraud, for instance, it's not uncommon for a senior employee in a trusted position to collude with the criminals. For this reason, firms need to look carefully at their auditing processes and may want to consider digitising elements of procurement, including contracting, buying and invoicing.

If business fraud does indeed rise sharply this year, it will happen as trading conditions deteriorate for many companies. They must therefore act promptly to ensure that they are as well prepared as they can be for the coming challenges, McKenzie warns.

"A pinch of prevention is worth a pound of cure, especially when it's all too easy for fraud losses to run into many thousands of pounds," she says. "The hassle and heartache of falling victim to a scam is the last thing that small firms need at the moment."

RECESSIONS TEND TO TRIGGER A RISE IN FRAUD

Change in GDP versus change in the number of fraud cases in selected recessions



University of Portsmouth Centre for Counter Fraud Studies, 2020


Busà Photography via Getty Images

“It’s likely that what we know about the criminal use and abuse of non-financial industries is just the tip of the iceberg

MONEY-LAUNDERING

The welcome mat of the UK’s laundromat

Although the financial services industry is well versed in anti-money-laundering practice, estate agents, art dealers, jewellers and the like are far less competent. Together, they constitute a large weak spot that criminals are targeting

Fiona Bond

Money-laundering is very big business. While the clandestine nature of the crime obviously makes it difficult for the authorities to gauge its scale with great accuracy, the United Nations Office on Drugs and Crime estimates that a sum equating to between 2% and 5% of the world’s GDP is laundered each year.

The statistics make particularly sombre reading for the UK, which is the second-biggest hotspot for money-laundering after the US, processing an estimated £88bn in criminal funds annually.

The domestic financial services sector has, unsurprisingly, been the focus of regulatory attention, with the Financial Conduct Authority imposing several hefty fines on banks for anti-money-laundering (AML) failures in recent months. But the criminals, whose methods are becoming ever more sophisticated, aren’t merely targeting big financial institutions to use as vehicles for shifting dirty money.

The Basel Institute on Governance, an independent organisation dedicated to financial crime prevention, has warned that lawyers, estate agents, casino owners, art dealers, precious-metal traders and other non-financial professionals are significantly more susceptible to money-laundering.

Kateryna Boguslavska works for the institute as a project manager on the *Basel AML Index*, its regular assessment of money-laundering risk around the world. She reports that, despite “limited and localised progress in some areas, the non-financial sector could be considered vulnerable in most countries”.

Boguslavska explains that there are three key reasons for the sector’s vulnerability: its limited understanding of its AML obligations (and of money-laundering generally); its poor implementation of AML procedures; and its lack of effective supervision by the authorities.

Take the property sector, for example. Noting a significant inflow of cash to the UK market from foreign sources, a damning report published by the government in 2020 uprated the money-laundering risk in the real-estate sector to high. And, despite the introduction of the Economic Crime (Transparency and Enforcement) Act 2022, buyers continue to circumvent the rules. Approximately 52,000 properties around the country are owned anonymously, according to Transparency International UK.

“We strongly support more transparency around who owns UK property and we welcome the changes introduced by the act, including the register of overseas owners,” says Ian Fletcher, director of policy at the British Property Federation. “But further changes are needed to bring companies owned through trusts into the rules, so that the legislation works as intended.”

Both the authorities and vulnerable businesses in the non-financial sector should be working harder to shore up their defences, argues David Lewis, managing director and global head of AML advisory at risk consultancy Kroll.

“There’s a dismal level of engagement from the non-financial sector, while little or no effective risk-based supervision and enforcement action is taking place where deficiencies are found,” he says. “It’s likely that what we know of the criminal use and abuse of non-financial industries is just the tip of the iceberg.”

International watchdog the Financial Action Task Force has come up with a long list of recommendations to serve as AML standards, many of which are concerned with due diligence. In its simplest terms, know-your-customer (KYC) due diligence means sourcing information to verify a customer’s ID, understand the nature of their activities and assess the risk they present – for instance, by screening for sanctioned individuals and ensuring that higher-risk customers are subject to enhanced checks. A robust KYC framework requires the continuous monitoring of customers.

Although KYC practice may be standard in the financial services industry, this is an entirely new activity to many other sectors, whose understanding of money-laundering may be limited.

Colum Lyons is the founder and CEO of ID-Pal, a provider of identity verification systems. He says: “This might surprise many people, given how often we’re asked to provide some type of identity information, but the latest and best form of verification tech is still in its infancy.”

Lyons advises non-financial firms to learn from the way financial service providers have “fully adopted the right processes. Compliance with AML and KYC is neither just a checklist to be completed, separate from day-to-day operations, nor a concern of only some of your team. Fraud prevention should be at the core of any business that wants to protect its reputation, revenue, customers and other stakeholders.”

Future technological advances, such as machine learning, promise to streamline KYC processes, enabling users to analyse data far more quickly and cost-efficiently. Secure platforms that help businesses to meet all their compliance needs in one place, from AML regulation to the Data Protection Act 2018, will become the norm too.

While there is growing pressure on non-financial businesses to do better, it’s widely agreed that the regulators also need to up their game and do more to help them.

“These supervisors need to be properly resourced, equipped with the appropriate legal tools and empowered to supervise on a risk-based approach,” Lewis says. “This is the international standard all countries have agreed to – they just need to commit. Until they do, legitimate businesses will continue to incur increased costs and our economies will continue to suffer.”

52,000

UK properties are owned anonymously

The transaction threshold above which art dealers have to demonstrate AML processes is

€10,000

32,440

offshore companies hold land titles across the UK

Transparency International UK, British Art Market Federation, 2023

Fighting the soaring cost of policy abuse in ecommerce

Online shoppers demand generous policies on issues such as returns, but these facilitate mounting abuse and fraud. Merchants need to act

With online retailing becoming ever more competitive, merchants have changed their policies in areas such as returns and refunds to become more shopper-friendly. These drive customer growth and retention – but are also fueling mounting abuse.

Some abuse is from genuine consumers engaged in so-called “light fraud”, such as returning clothing after wearing it once, known as “wardrobing”, or creating a new email to benefit from a referral bonus.

But online retailers are also increasingly targeted by career fraudsters and criminal gangs who may perpetuate abuse on a much larger scale, lodging bogus item-not-received (INR) claims on multiple expensive items or shipping empty boxes back for a refund.

Resellers may also capitalise. They use multiple accounts to scoop up the supply of limited-availability items or abuse discount codes to flip high-demand goods for a profit. This damages customer experience and leaves a retailer potentially competing with its own discounted stock.

The problem is made more acute by opportunistic customers and fraudsters networking online, swapping intelligence on tactics and easy targets. They may identify retailers that, for instance, are not effectively reconciling returns with card chargebacks, making it easy to receive two refunds for one returned item, known as “double dipping”.

Joe Gelman, a product marketing manager at Riskified, a leader in ecommerce fraud and risk intelligence, comments: “The inventiveness is endless.”

This inventiveness is reflected in the data. The National Retail Foundation projected that in 2022 some $22.8bn would be lost to fraudulent online returns in the US alone.

A survey by Riskified in November found that 45% of online shoppers admitted some kind of return fraud or policy abuse. Many rationalise their behaviour: 27% said they only do it with large retailers, and 14% felt “owed” because of a poor customer experience.

As well as the immense financial cost, policy abuse causes many other problems, such as skewing key performance indicators. For example, a trial promotion may appear to have brought 1,000 new customers, but in reality it may be a tight ring of resellers using multiple one-time accounts. Based on the apparent success, a merchant could launch a new promotion-based strategy that compounds their losses.

There is also the wasted time and expense of handling and investigating claims and cases, plus the risk that a good customer may accidentally be categorised as an abuser. This could cost the retailer not only that customer but likely their friends and family too.

However, retailers cannot simply rewind to the more restrictive policies of a decade ago. A study by Appinio in 2022 found that 80% of UK online shoppers regard free returns – a policy that facilitates wardrobing – as very important. In Germany, 72% of online shoppers said free returns were very important, much higher than, say, the 38% who cited next-day delivery.

The largest ecommerce giants have reset customer expectations at an elevated level, raising competitive pressure on all other online vendors. Although some high-profile clothing retailers have introduced more restrictive returns policies, for most merchants a package of no-quibble refunds, free or discounted returns, and promotional codes are essential elements of their offering.

The problem for merchants is that consumers and fraudsters can both evade detection by setting up multiple accounts. Most shoppers have a wallet or purse full of credit cards and can set up a new email in minutes; this makes creating multiple accounts straightforward and means merchants struggle, for instance, to prevent consumers from enjoying repeated introductory discounts.

Basic checks are even less effective against resellers and professional fraudsters, who may also use proxy servers or other techniques to ensure their army of accounts have different IP addresses. They may use other methods to hide their tracks, such as changing keyboard or language settings between creating accounts.

Gelman says: “The only way to really deal with policy abuse is to get to the root of the problem. And that’s figuring out where all of these patterns are originating from and going back to the source.”

Riskified’s Policy Protect implements this to put the merchant back in control. Gelman explains that the platform runs through every account, determining all possible connected pairs, then mapping out how each of these pairs overlap and interconnect. A further process deploys proprietary machine learning to identify clusters of accounts that are, in reality, controlled by a single source. This immense data-processing exercise uses not only the merchant’s data but the vast pool on the Riskified platform (processed in accordance with all relevant legislation).

Once the platform has identified the real patterns behind multiple accounts, the merchant can start making informed decisions through an automated dashboard. For instance, it can ensure one-time codes are used once per customer, reducing promotional costs. At the other end of the scale, it helps merchants identify the patterns of item-not-received and empty-box returns that are characteristic of systematic abusers, patterns that may be much harder to spot at the level of individual accounts.

Gelman says that most online retailers will, at present, have no idea of their losses from the various forms of abuse and fraud until they have this level of visibility. For instance, a UK activewear brand which worked with Riskified discovered that 15% of all returns were abusive.

More generally, some merchants have been able to detect 95% of resellers and reduce promotional costs by up to 70% by thwarting misuse of coupons and codes, while still offering them to genuine customers.

Gelman says online merchants must act now to escape their difficult position. “There is a real urgency and pain on policy abuse,” he says. “Merchants are watching their margins and struggling to compete. But they can’t pull back these policies because consumers demand them.”

45%

of online shoppers admitted some kind of return fraud or policy abuse

27%

said they only do it with large retailers

14%

felt “owed” because of a poor customer experience

Riskified, 2022

“The only way to really deal with policy abuse is to get to the root of the problem

For more information, visit riskified.com/policy-protect

riskified

INSIGHT

'The need for a consistent approach has never been greater'

Financial institutions must get better at cooperating – both internally and externally – to mitigate the risk of cyber attacks, argues ORX's **Roland Kennett**

If you look at any survey of financial institutions, you'll find that cybersecurity will generally feature at the very top of the list of material and emerging risks they're most concerned about. In our highly digitised world, that shouldn't come as a great surprise. In fact, it has been the case for a very long time.

Cyber incidents are defined by the UK's National Cyber Security Centre as "a breach of a system's security policy in order to affect its integrity or availability, and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990)". They happen with an incredibly high degree of regularity. Perhaps the most eye-catching recent incident was the prolonged attack on Costa Rica by cybercrime group Conti.

So why, given all of this, do banks and insurers still struggle to quantify their exposure to cyber risk?

Part of the issue is organisational. There is a difference between the technical teams that ensure an organisation is properly protected and the risk professionals who work to calculate its exposure. The data sets that are needed for both activities tend to be different, even though they share a common basis. Most focus has – correctly – been on prevention, but the consequence is that it is very hard to pull together the data needed by risk professionals for calculating exposure.

What's more, the frameworks (language, system and process) that have arisen on either side are not aligned, which has led to a siloed approach. Many systems have been developed, several of which have different attributes. The terminology varies and information can often be contradictory too. This means that different stakeholders find it hard to gain a common understanding, while those trying to measure exposure often face the time-consuming task of scouring numerous sources of data for something usable.

If sharing consistent data is a challenge internally, this is increased tenfold when it comes to sharing across the industry. But the need for a consistent approach has never been greater. Cybercriminals are continually seeking new ways to achieve their ends. They know they have to get it right only once to win, while organisations have to get it right all the time to stay protected. That makes it hard for firms to stay ahead of the threats.

We have a risk management conundrum: here is a risk, which everyone is talking about, that's being heavily invested in, yet there is little data to justify that investment. How can it be resolved? Internally, companies must continue with their work to standardise terminology and systems so that all functions are receiving the information they need. Externally, we must continue developing industry resources that enable firms to benchmark themselves against their peers.

Part of the solution lies in data sharing. In 2020, ORX created ORX Cyber – a service where more than 25 financial services firms from around the world swap data concerning cyber losses, controls and indicators. This exchange has two main benefits. First, participants can start to see how their experience of cyber risk events compares against the aggregate peer-group data. But second, and perhaps more crucially at this stage, it's also meant that they have had to start sourcing data from within. This in turn is forcing them to hold internal discussions about what material is needed and why.

Data sharing is only one aspect of the solution, though. In our experience over the past 20 years, collaboration has emerged as the best defence against cyber threats. Bringing experts together to share their expertise and knowledge can help financial institutions to make rapid progress together, rather than as individuals. This 'wisdom of crowds' approach to tackling big issues can make all the difference.

The threat of cyber incidents will undoubtedly remain at the top of our risk lists. But the more we collect better data and collaborate, the more we can start to quantify it – and then justify the investment decisions we are making. ●

Roland Kennett
Membership director, ORX

Tom and Steve via Getty Images

LEGISLATION

Westminster's washeteria war

Having reclassified fraud as a national security threat, the government's resolve against financial crime – particularly money-laundering – is hardening. But will the new measures it's considering go far enough?

James Gordon

The City of London Corporation's website boasts of the UK's status as "the world's most global financial centre", but what it doesn't mention is that the country is also a magnet for international financial crime. The problem has grown to such an extent that the government announced last month that it was classifying fraud as a national security threat – a move that UK Finance, the trade body representing the financial services sector, had been calling for since September 2021.

Nick van Benschoten is a director at UK Finance who leads its work against international illicit finance. He explains that the reason for fraud's reclassification is that it's "endemic in the UK and often linked to other forms of financial crime, such as money-laundering, corruption and the financing of terrorism".

Money-laundering is a particular sore point. This alone costs the UK economy £100bn a year, according to the National Crime Agency.

Russia has been the source of much of the dirty money. Graeme Biggar, director-general of the National Crime Agency, indicated the extent of the problem when he told the Treasury select committee in 2021: "We have done some analysis recently on some of the laundromats that have come out of Russia and the former Soviet Union. A disturbing proportion of the money that comes out of them – not much shy of 50% in one case – was laundered through UK corporate structures."

According to the parliamentary intelligence and security committee, oligarchs were allowed to recycle "illicit finance through the London laundromat" with virtual impunity for many years until Russia's invasion of Ukraine in 2022 finally drove the government to sanction individuals with links to the Putin regime and freeze their assets. In rushing through the Economic Crime (Transparency and Enforcement) Act 2022 last March, the government required "foreign owners of UK properties to reveal their true identities", but many MPs and legal experts believe that the legislation could – and should – have gone a lot further.

> "If we really want to combat financial crime, the government will need to establish a single command structure with an annual budget of about £250m

Two all-party parliamentary groups (APPGs) – one on fair business banking and the other on anti-corruption and responsible tax – published an *Economic Crime Manifesto* in May 2022. This document argues that the act should be amended so that, as well as creating a register of foreign property owners, it tightens the rules governing shell companies (which it calls "the money-launderer's best friend") and makes some significant changes at Companies House.

The government has taken the APPGs' recommendations on board, so at least some of these are likely to be incorporated in the economic crime and corporate transparency bill, which is set to be enacted this summer (see page 14). Despite this, Professor Marc Moore, chair in corporate and financial law at University College London, doubts that the proposed changes would have the desired effect.

"Even wholesale reforms of Companies House are unlikely to make a difference," he argues. "A huge proportion of shell companies that are set up to perpetrate fraud and other crimes are incorporated overseas, so they won't fall within the remit of Companies House or the UK courts. I'm therefore not completely hopeful, in the absence of cooperation from registrars in those other jurisdictions, for reforms of this nature."

Helena Wood, who heads the UK economic crime programme at the Royal United Service Institute's Centre for Financial Crime and Security Studies, is more optimistic.

"While the UK is not the only net exporter of shell companies, a sizeable number of those listed in the Panama, Paradise and Pandora papers were British. Providing that Companies House is properly resourced to vet who's coming through the front door of our corporate registry, I believe that the bill will have a significant impact on stymieing economic crime," she says.

Wood does agree with Moore that the legislation won't "entirely eliminate the use of shell companies to conceal illicit finance. There are several tiny islands that have based their economies on this business model, so they won't be stopping any time soon. Yet I believe that the UK's decision to clean up shop will create more transparency in international finance. In time, that alone will shine more of a spotlight on the shady practices of shell companies operating from far-flung locales."

Is there a case for an outright ban on the use of shell companies?

"In an ideal world, legislators would certainly consider such a step," Moore says. "But the reality is that it's hard to distinguish legally between the legitimate use of a limited-liability partnership or subsidiary company and a shell company arrangement. Many bona fide businesses set up subsidiaries for perfectly legitimate reasons. To shut down a shell company that's being used to launder money, for instance, requires determined investigation – and not all jurisdictions have the will and/or resources to do so."

Moore's last point highlights the need for a properly funded and coordinated enforcement effort. If this is lacking, any number of legislative reforms won't improve the situation.

"It will require a transnational approach," he says.

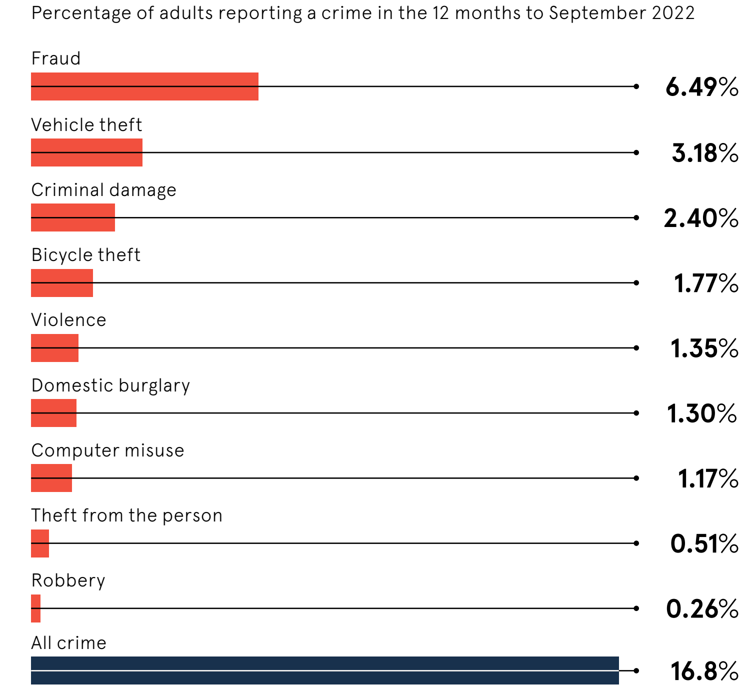
Wood agrees, arguing that "a far broader and more ambitious reform of UK economic crime policing" will also be vital. She adds: "If we really want to combat financial crime, the government will need to establish a single command structure with an annual budget of about £250m."

And the opportunity cost of failing to do so? Van Benschoten outlines the likely ramifications if the crime-fighting agencies aren't given the right legal powers or the resources required to wield these effectively.

"Failing to take a robust approach across the whole economic crime landscape will jeopardise the UK's global reputation as a facilitator of convenient, fast, diverse and competitive markets," he warns. "The markets require proper controls, which engender trust. If trust in our financial system ebbs away, there is a risk that those markets will clog up. As a result, this country might lose not only its competitive edge but also its reputation as a safe, transparent economy." ●

FRAUD IS BY FAR THE MOST PREVALENT TYPE OF CRIME REPORTED IN ENGLAND AND WALES

Percentage of adults reporting a crime in the 12 months to September 2022



Office for National Statistics, 2023

GEOPOLITICAL RISK

Sanctions – a compliance headache for British SMEs

Much of the West has had sanctions in place against Russia for 12 months. For many smaller businesses, the task of operating within these complex and wide-ranging rules is proving onerous

David Stirling

If they want to ensure their compliance with the government's ever-burgeoning sanctions rules, small and medium-sized enterprises in the UK will need to move 'staying alert to emerging geopolitical risks' much higher up their to-do lists.

"SMEs have to expand their geopolitical knowledge if they want to stay ahead," argues Joel Lange, general manager of risk and compliance at Dow Jones. "These rules no longer just affect global banks."

The use of sanctions is not new, of course, but the sweeping restrictions imposed on Russia after it invaded Ukraine in February 2022 represent a paradigm shift. They included asset freezes and travel bans for oligarchs, including the then owner of Chelsea FC, Roman Abramovich, as well as known allies of the Putin regime. Russian bank assets in the UK were also frozen; Russian state-owned and key strategic private companies were banned from raising finance in the UK; and trade and export controls were introduced on goods such as military tech and even jewellery.

By early February 2023, the government had sanctioned more than 120 businesses and 1,200 people since the invasion of Ukraine. Unsurprisingly, this has had an indirect impact on many British businesses.

All UK firms are required to comply with the sanction rules, which ban transactions with – or the provision of financial services to – any sanctioned entity. That means more screening, to check whether you or your clients interact with people or businesses on the sanctions list. A failure to abide by the rules could lead to a fine from the Office of Financial Sanctions Implementation or even a prison term.

"Due diligence has undoubtedly become more time-consuming, particularly for those SMEs with fewer resources," Lange observes. "There is a need to evaluate not only your own business exposure but also those of suppliers, third parties and agents. Checking names on a list can be straightforward, but this task has become challenging given the sheer number of names involved. And, even though it may be clear whether you have a direct business link, where do you stand if you're renting a building from a sanctioned individual, say? Are you allowed to pay them rent or not? There has been a spike in the number of queries to the regulators about such issues."

Immediately after the invasion, the small fintech firm IFX Payments took decisive action to enforce specific controls and freezes on Russian and Belarusian payment routes.

"We didn't have huge amounts of payments to and from Russia and firms dealing in the rouble, but there were enough to have an impact on the business," explains Tony Brown, the company's head of compliance and money-laundering reporting officer. He adds that 24/7 monitoring of both sanction lists and payments has since led IFX Payments to treat other countries with greater caution.

> There are certain components that go into a digger which also go into a guided missile. Will a digger-maker have to employ an in-house sanctions specialist?

The imposition of more than 10,000 international sanctions last year resulted in empty shelves in Russia

"We saw more payments being made in states with close financial ties to Russia, such as Moldova and Cyprus. Every payment was flagged for manual review and couldn't be released until a compliance specialist had looked at it," Brown explains. "Sanctions are nothing new – but they've never before come at this scale, speed or complexity."

With these factors in mind, IFX Payments is training a member of its in-house compliance team to become an expert in sanctions.

"The compliance industry has long focused on anti-money-laundering, so there's a big knowledge gap when it comes to understanding sanctions," Brown says. "I've seen CVs stating experience of sanctions screening, but there is a finite number of real sanctions specialists studying global economic and political trends."

Many SMEs will struggle to fill this gap, he says, adding: "There are certain components that go into a digger which also go into a guided missile. Will a digger-maker have to employ an in-house sanctions specialist? It will find that really difficult."

Lange observes that, even with an expert on board, the compliance burden will still be onerous.

"This huge spike in sanctions means that SMEs need to decide whether they have enough resources dealing with them and in dialogue with regulators," he says. "They must prepare for the possibility of more sanctions on nations such as China too. New supply chains and counterparties are also emerging around the world as a result of the Russian invasion and Brexit. You can't just say 'we don't deal directly with Russia or China so we're fine' any longer."

Chrisol Correia, global head of financial crime risk management at risk tech specialist Facctum Solutions, adds that the situation is only likely to become more complex.

He says: "The perception of the risk has grown significantly. Will governments use this increasingly as a geopolitical tool, meaning that sanctions lists get bigger and bigger? Do we take the risk of onboarding a client just to offboard them again if the risk profile continues to change?"

Although businesses are expected to have adequate systems to manage compliance, as well as a person of sufficient authority to oversee this, some SMEs may want to consider using external expertise, which can often provide specialised data feeds for sanctions screening.

Lange says that Dow Jones "can aggregate all the data cohesively, so our SME customers can check themselves and their suppliers against it".

Crucially, this must be done under the overall control of the SME. Third parties can provide all the information, but they cannot be held responsible for any decisions based on it.

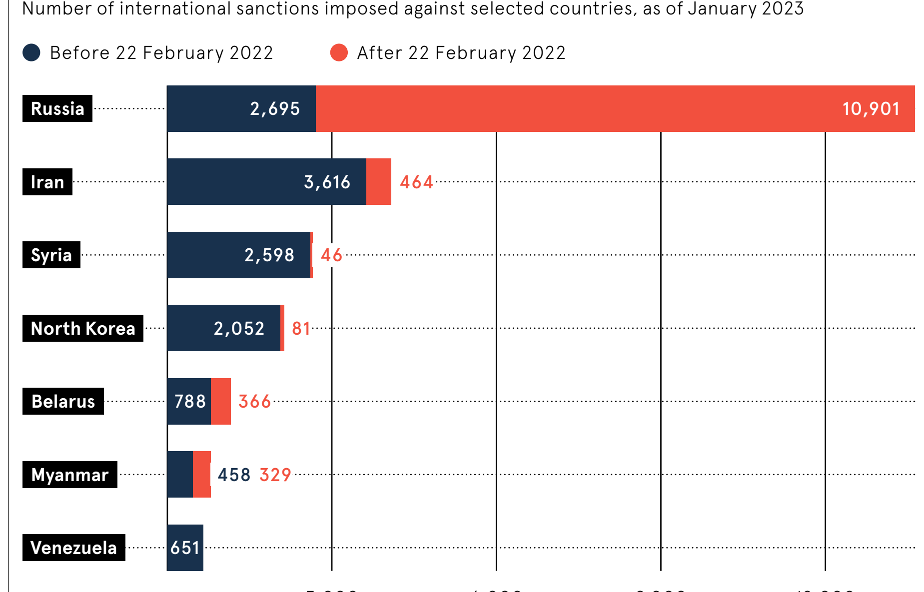
"SMEs are in a difficult situation: they can't afford the skills they need, but they can't outsource responsibility," Correia says. "It would be good if they were allowed to use external expertise in decision-making."

Brown offers one final consideration: that whoever in a firm is ultimately responsible for compliance must keep in mind the ethical aspect of sanctions and take this seriously.

"Sanctions are not just about oligarchs. This issue is about civilians getting killed," he stresses. "There's a human face to it." ●

RUSSIA TOOK A HUGE HIT FROM SANCTIONS AFTER ITS INVASION OF UKRAINE

Number of international sanctions imposed against selected countries, as of January 2023



Castellum.AI, 2023

Commercial feature

How automating KYC can reduce regulatory risk and boost productivity

Traditional KYC processes are cumbersome, delaying client onboarding and potentially resulting in lost business. Automating KYC can speed up this process, reduce errors and give financial services firms more flexibility to manage the downturn, says Encompass's KYC transformation director Howard Wimpory

As the UK economy slows and financial services firms face a potential squeeze on profitability, accelerating digital transformation plans to boost efficiency and reduce costs is more important than ever.

While firms typically scale back spending in times of economic stress, investing in digitisation now means firms will feel the benefit once the economy picks up again. One area of digital transformation that has received less attention is know-your-customer (KYC) technology, often because investment in fraud and financial crime-prevention tools has typically focused on software that flags suspicious payments.

Investing in KYC automation tools can not only reduce regulatory risk, it can also help improve revenue generation by accelerating the onboarding process, while also boosting productivity by reducing the amount of manual tasks KYC analysts are expected to complete.

The challenges with traditional manual KYC processes are fourfold. First is cost. Manual KYC work relies on a shrinking pool of experienced talent, which is making it more expensive to hire good analysts.

Second, the KYC process is also becoming more complex. Regulators have imposed tougher KYC rules, making it harder for banks to maintain compliance. That complexity extends beyond onboarding to ongoing monitoring of customer behaviour.

Third is client experience. KYC has historically been the least positive experience a client has with a bank. Manual KYC checks for companies during onboarding can be a slow process, taking anywhere between 60 and 90 days to complete. In today's fast-paced world, where digital-only new entrants can sometimes onboard clients in a matter of minutes, waiting months to open a bank account is no longer tolerated.

Finally, there are the consequences of manual KYC processes if things go wrong. Banks risk landing hefty financial penalties for KYC failings, which can also lead to reputational damage. The consequence of poor client experience can manifest either in delayed revenue flow (because it takes too long to onboard new clients) or revenue being lost altogether (because clients abandon the onboarding process and switch to a competitor who can open an account faster).

The implications of those manual processes can be felt across a bank's potential client base. SMEs are unlikely to be patient given that if they don't have a functioning bank account, they can't run their business. For larger businesses that, say, want to carry out trading activity through an investment bank, they want to be able to make trades fast. Having to wait too long for the onboarding process to be completed means the trading opportunity will likely have passed, and they will just take their business elsewhere.

> Technology reduces costs, ensures regulatory compliance and improves client experience by making onboarding faster

Reducing manual processes with technology can help financial services firms solve all four of these pain points. To start with, technology can significantly improve the risk detection process – and it can do it consistently. No matter how good an analyst is, if they are inundated with work, suffering fatigue or in some other way distracted, there will be fluctuations in quality. Technology, on the other hand, can identify risk in a consistent way within set parameters regardless of how many cases it must process.

Technology can also allow low-risk cases to be automated without any human intervention, while flagging higher-risk or complex cases that require analysts to dig deeper. Smart technology can identify those issues faster, while also using AI and machine learning to make accurate, human-like decisions.

Technology therefore reduces resource costs, ensures regulatory compliance, improves the client experience by making onboarding faster, and helps avoid the potential financial and reputational hit of getting manual KYC processes wrong.

To get on the front foot with these trends, financial services firms need to constantly evaluate their processes and assess whether they remain effective as the environment changes via new regulations or shifts in client expectations. If firms are not constantly reviewing their processes and identifying gaps or weaknesses, then their operations will quickly become outdated.

That also means firms need to make sustained investment in technology that can address those gaps. Historically, firms would try to solve increases in KYC caseload by throwing more resources at the problem. That might provide a temporary fix, but the fundamental issue which is causing those capacity issues is not addressed. Instead, firms must re-engineer their processes to become more productive, with technology doing the heavy lifting by discovering risk faster and more directly.

Using KYC technology like Encompass's automated corporate due diligence platform, the process of identifying the ultimate beneficial owner of a company can be whittled down to less than 10 minutes – something that could have taken hours or even days to complete manually. That time saving means analysts no longer have to spend the majority of their working hours hunting down information. Instead, analysts can spend their time making sense of the information that is presented to them and potentially identifying inter-related parties that may not have previously been clear. In the past, that would require resilience and energy to keep looking, often against the backdrop of tight deadlines. The upshot: cases were not examined to the depth needed. Technology ensures no stone is left unturned—and it does it in a fraction of the time.

With pressure on back-office teams to be more efficient, adopting such technology can do two things. First, faster KYC processes speeds up the onboarding process, which translates into faster income generation and reduces the risk of potential new clients moving elsewhere – a direct economic benefit to the bank. Second, automating KYC processes increases productivity by freeing up spare capacity. That gives financial services firms more flexibility about how to allocate their resources, either by reducing the number of analysts needed or enabling analysts to handle a greater volume of work. All of that can help better position financial services firms for the economic recovery and ensure they are set up for long-term growth.

Find out more at encompasscorporation.com

encompass
the full picture, fast

GETTING TOUGH ON PHISHING

Our reliance on digital communications tech is playing into the fraudsters' hands. Data from the Office for National Statistics indicates that half of all adults in the UK received at least one suspected phishing attempt via an email, text or social media message in the past month. And when a phishing attack on a company hits home, it will cost that firm an average of $4.65m (£3.88m), according to IBM. But businesses are fighting back: a significant number are backing up their data security training for staff with robust sanctions – including fines or even dismissal – for anyone found to have shirked their responsibilities. It's a radical approach, but will it work?

42% of UK organisations fine employees who expose them to phishing attacks (the global average is 26%)

1 in 4 UK firms would be willing to dismiss an employee for a phishing mistake

70% of firms that have disciplined employees for phishing mistakes feel that this has increased awareness of cybersecurity among the workforce

MOST EMPLOYERS WORLDWIDE TAKE SOME FORM OF DISCIPLINARY ACTION AGAINST WORKERS WHO EXPOSE THEM TO PHISHING ATTACKS

Percentage of IT professionals giving the following responses to the questions: does your firm take disciplinary action against employees who fall for phishing attacks? If so, what form would that take?

Yes	No
55%	45%

Form of disciplinary action	%
One-to-one discussion with manager	60%
Discussion with the cybersecurity team	59%
Impact on the employee's performance review	52%
HR-enforced disciplinary action	45%
Removal of access to systems	35%
Monetary penalty	26%
Dismissal	18%

EMAIL-BASED PHISHING IS THE MAIN FOCUS OF DATA SECURITY COURSES, YET LITTLE TIME IS DEVOTED TO SUCH TRAINING

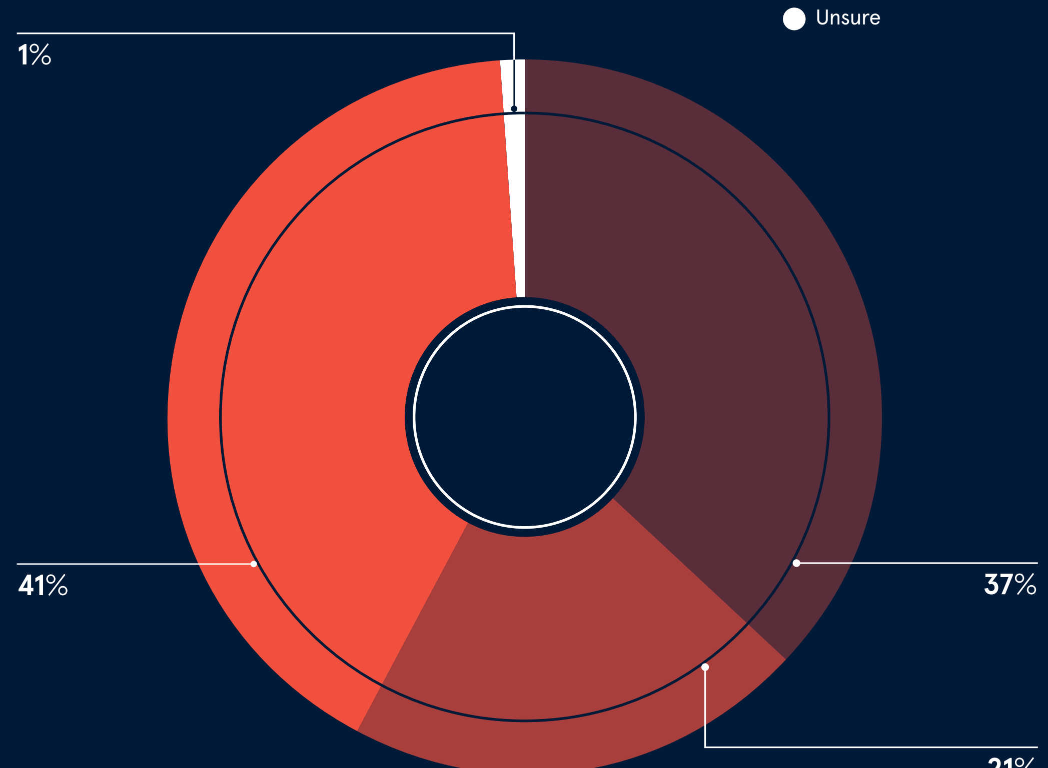
Share of IT professionals worldwide citing topics covered by their firms' awareness courses, plus the average time spent by employees in such training each year

Topic	%
Email-based phishing	49%
Malware	47%
Wi-Fi security	44%
Ransomware	43%
Mobile device security	43%
Password best practice	42%
Best practice for internet safety	40%
Invoice fraud	40%
Cloud-based threats	39%
Best practice for remote working	37%
Physical security measures	36%
Compliance-related topics (eg, GDPR)	33%
Insider threats	33%
Multi-factor authentication	32%
SMS-based phishing	26%
Voicemail-based phishing	23%

Up to 30 minutes	30 minutes to 1 hour	1 to 2 hours	2 to 3 hours	More than 3 hours
9%	29%	37%	12%	13%

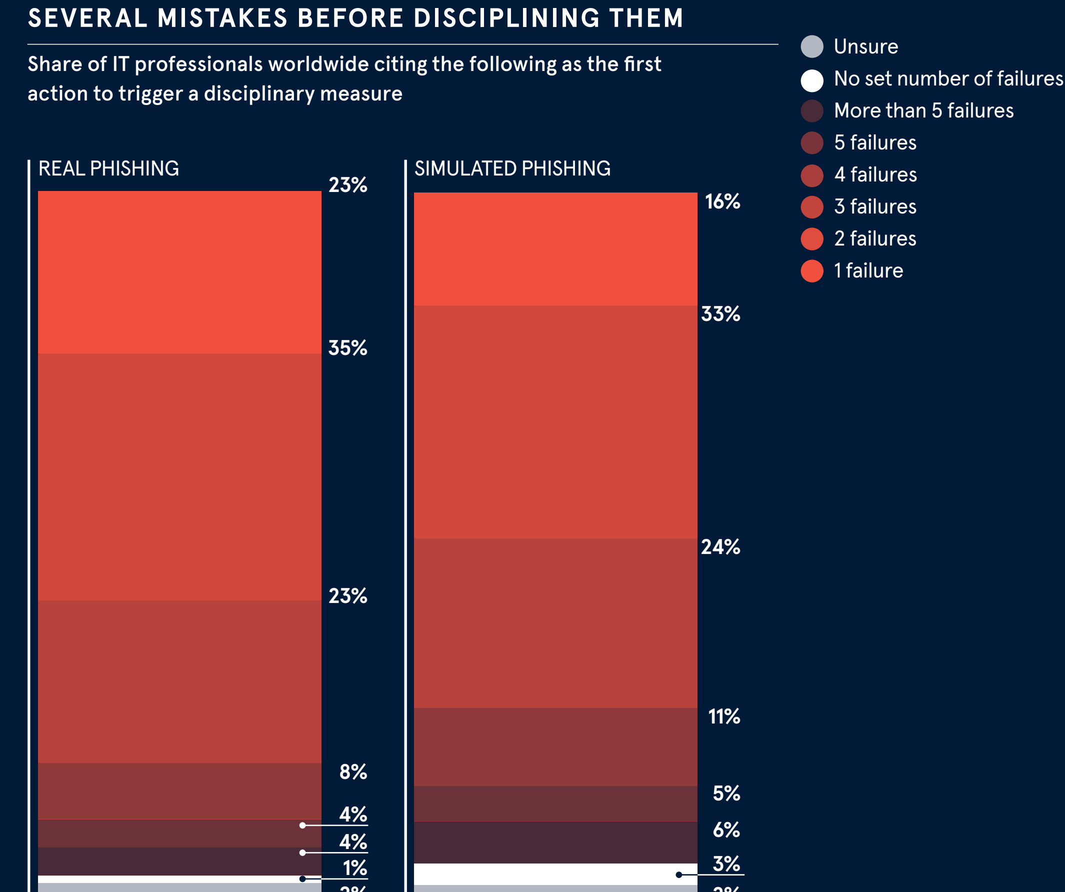
WORKERS HAVE MIXED FEELINGS ABOUT THEIR EMPLOYERS' POLICIES ON PUNISHING PHISHING MISTAKES

Share of workers worldwide giving the following responses when questioned about their employer's phishing disciplinary policy



SOME EMPLOYERS LET REPEAT OFFENDERS MAKE SEVERAL MISTAKES BEFORE DISCIPLINING THEM

Share of IT professionals worldwide citing the following as the first action to trigger a disciplinary measure



Proofpoint, 2022

INTERVIEW

‘This is a community-led and community-owned effort’

An innovative sector-wide network is breaking down silos surrounding user data to spot criminal behaviour. This is already achieving useful results, as one of its prime movers, **Clarence Chio**, explains

Laurie Clarke

There has been plenty of talk in recent years about how neobanking has upended the traditional finance world. But the latest crop of fintech challengers is still struggling with an age-old problem: fraud.

Over the past few years, neobank N26 has been fined for having “weak” anti-money-laundering (AML) systems; Monzo Bank has been investigated in a money-laundering probe; car rental firms, hotels and other companies have banned their customers from paying them using CashApp and Chime because of fraud concerns; and investment app Robinhood has suffered significant losses to fraud.

Innovations such as machine learning have been hailed as a potential salve, but there’s a back-to-basics method that could help too, according to a new group of fintech reformers: sharing intel.

“A pattern that we’ve seen since the beginning was that the companies we worked with wanted to learn what others were seeing in terms of fraud,” says Clarence Chio, co-founder and CTO of Unit21, a risk and compliance infrastructure platform that’s a member of this new group. “But there wasn’t a solution that helped them to do that.”

Financial consortia that exchange information on fraud risk have existed in the traditional finance sector for decades. But fintech firms, neobanks and crypto companies deal with a slightly different set of risks. One day, Chime’s co-founder and CTO, Ryan King, pointed out to Chio that Unit21 already held the user and transaction data of more than 100 fintech companies – planting the seeds of an idea for a new kind of consortium. Soon afterwards, Unit21 set up the Fintech Fraud DAO, a decentralised autonomous organisation comprising fintech businesses that swap their user data in an effort to identify and stop fraud before it can spread.

The DAO lets participating organisations share aggregated user data through an open-source platform, aiding the rapid identification of suspicious activity and helping to overcome the fact that traditional AML and know-your-customer systems are not designed for data-sharing at the scale required to effectively prevent fraud. Participating firms include Airbase, Brex, Chime, PrimeTrust and Yotta.

Typically, neobanks have not had much incentive to share their data, largely because they wouldn’t want a competitor to extract marketing intelligence from that material, Chio says. But he adds that this inherent fear is being outweighed by their desire to learn from others – especially as fraudsters tend to be very persistent repeat offenders.

> **If participants don’t respond to the signal within a short time frame, they stand to lose 10% more to fraudsters**

“The same criminals are targeting everyone, not just one company,” he says. “And they go after the lowest-hanging fruit.”

Unit21 incorporated a distinct entity to operate the consortium. Chio says this is because the firm didn’t want it to run on a profit-driven model, where the data could be packaged up and sold externally. This is where the idea for a decentralised autonomous organisation came in. The DAO works according to Web3 governance principles, where all participating companies own tokens that give them a stake in the network and allow them to vote on various matters. Participation in the DAO is free; firms simply have to agree to share their data.

“This is a community-led and community-owned effort, rather than something built by a vendor that we could have later gone on to monetise,” Chio says.

One of the most hotly debated issues in the DAO so far has been how to ensure data privacy. In a collective decision, the members chose to implement the same type of privacy mechanism often used by national healthcare systems and pharmaceutical firms: privacy-preserving record linkage. This is because sharing healthcare records incurs the same kind of privacy risks as sharing personal financial data. In the DAO, personally identifiable data is shared using a bloom filter (a probabilistic data structure based on hashing).

The way this works is that, if one participant is defrauded by, say, John Smith, it can tip off the others by sharing the tokenised form of his details with them.

“If they don’t already know who John is, the mechanism of tokenising his information makes it computationally impossible to generate the hashes,” Chio says.

This method means participants get an early warning about potential fraudsters among new sign-ups to their services. They receive a time stamp of all accounts across the sector – “something to the tune of ‘John Smith has been active in seven fintech firms in the past three weeks and has been blocked by five of them’”, explains a Unit21 spokesperson. This can tackle not only account takeover fraud but things such as so-called promotional abuse (where fraudsters join a service to take advantage of a promotional deal before exiting).

Chio cannot share data on how much fraud has been prevented by the consortium so far or how this rate compares against traditional methods. But he claims that about 20% of all the fintech data in the US flows through the DAO and that the group has already turned up some interesting findings.

Before working together, Chio and others suspected that the same fraudsters were targeting more than one financial services provider in the same way. Their hunch was soon borne out by the data: the DAO found that at least 10% of the fraud loss experienced by one participating firm had been experienced seven to 10 days earlier by at least one other in the consortium.

“This means that, if participants don’t respond to the signal provided by the DAO within a short time frame, they stand to lose 10% more to fraudsters, which could mean several millions of dollars,” Chio says. “That’s interesting validation for us, because there’d been no real way to prove this without any data-sharing between participants.”

The group started with its focus firmly on the neobank and crypto segments, he says. But it quickly attracted interest from traditional financial services too. When digging into why that was the case, the members realised that, for a lot of banks and credit unions, a steadily increasing number of their users are transacting in crypto or storing some money in neobanks. Cash flowing between these and traditional banks means the latter are getting exposed to the same risks.

“Banks have no real visibility over crypto sources or different online transacting methodologies because the traditional sources they use for risk don’t give them that signal,” Chio says. In the past five years, banks including Lloyds, NatWest, TSB and Virgin have taken steps to ban crypto transactions, but Chio believes that this will change.

“Traditional banks are starting to realise that they can’t take the most conservative route and block everything that they don’t understand indefinitely,” he says.

A number of traditional institutions have approached the DAO and asked whether they can buy the group’s data without joining, but it has refused. Instead, it’s working on pilots with two traditional banks with a view to bringing them into the fold. Although he can’t name them yet, Chio says they are regional banks that are operational in several US states. Each of them has more than $5bn (£4bn) in assets under management.

Crypto regulation is finally advancing in countries such as the UK and the US. But Chio sees consortia such as the Fintech Fraud DAO playing a potentially greater role in tackling fraud across the industry. He says that the crypto companies he works with are all eager for more regulation, because operating in a legal grey area is challenging. Even so, slow and patchy crypto regulation around the world means that motivating platforms to cooperate could prove a more fruitful way to legitimise their sector.

“Crypto companies will be incentivised to work together to clean this up”, he says, “just like the banking system was.”

$51m

The amount the average US fintech firm loses to fraud each year

Smaller fintech firms lose

57%

more to fraud than their bigger peers do, relative to income

46.5%

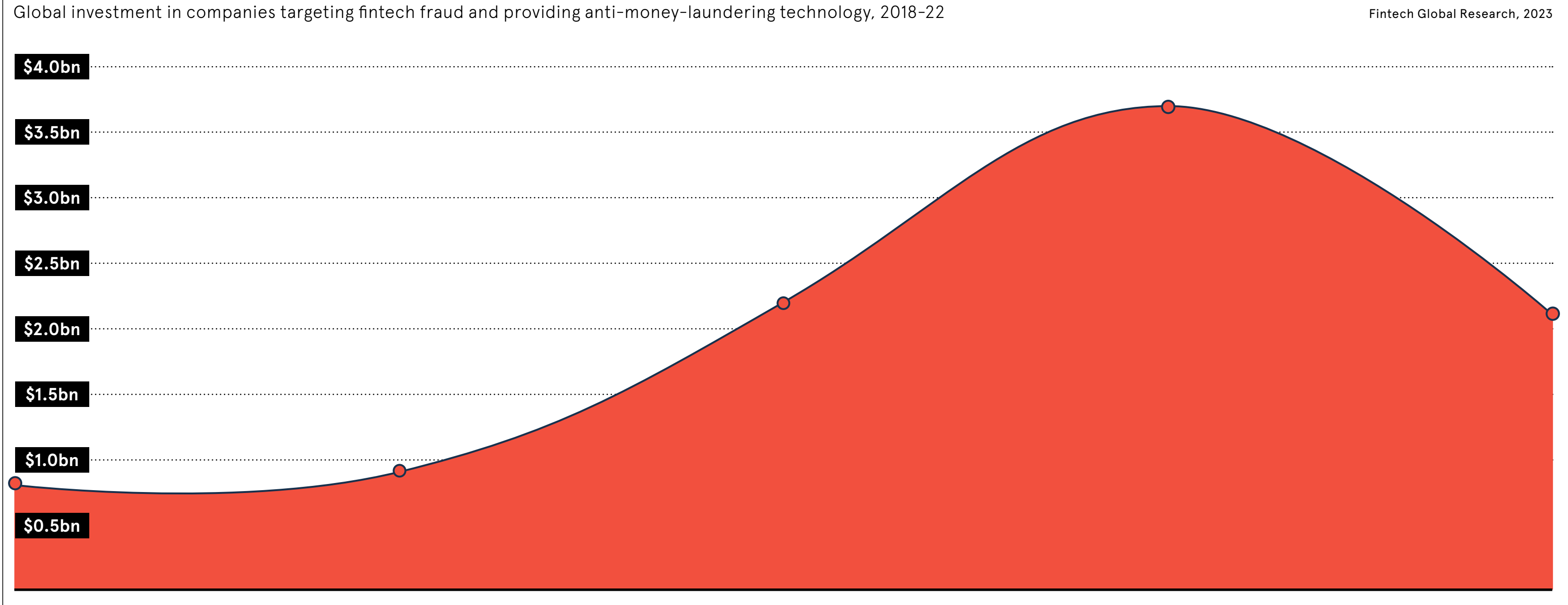
of fintech firms cite the cost of fraud as their biggest challenge

Pymnts.com, 2022

INVESTMENT IN FIRMS TACKLING FINTECH FRAUD DECLINED FOR THE FIRST TIME LAST YEAR

Global investment in companies targeting fintech fraud and providing anti-money-laundering technology, 2018-22

Fintech Global Research, 2023



Commercial feature

How better data can limit friendly fraud

For merchants, the holiday hangover is still here and the headaches are caused by illegitimate chargebacks – a so-called ‘friendly fraud’ that is anything but friendly

A couple of months on from the end of the frantic Christmas period, many merchants are suffering a holiday hangover.

This isn’t due to overindulgence in the leftover mulled wine. Instead, it’s the result of an overabundance of ‘chargebacks’: the process of returning money to consumers after a disputed transaction.

Most chargebacks happen within 60 days of the original sale, which means that, while the holiday season is long over, the chargeback hangover period is in full swing. Many merchants are suffering an excess of administration and a significant reduction in revenue.

Chargebacks: when fraud is friendly

While definitive figures are hard to find, chargebacks are clearly becoming more onerous in the digital age. So-called ‘friendly fraud’, which happens when customers make a purchase and then dispute the charge with their bank, is now the number one fraud attack affecting merchants.

In fact, it’s been calculated that friendly chargebacks might be responsible for between 40% and 80% of all ecommerce fraud losses.

This is a critical issue for merchants, who end up losing more than the cost of a sale. Chargebacks incur fees from the merchant – sometimes upwards of £150 per transaction – and administering them is time consuming.

Merchants who incur too many chargebacks can even be locked out of a digital payments system altogether for a period – a potentially fatal blow.

Old world solution

Monica Eaton, founder of chargebacks solutions company Chargebacks911, argues that chargebacks were once a legitimate tool, but have not kept up with the transition to a digital world.

“Chargebacks were a mechanism for consumer protection that really developed in the 1970s,” she says. “They make it very easy for consumers to ask for money back at the expense of merchants. This is an old idea for an old way of doing things.”

This “old way of doing things” was designed for a pre-internet world where payment cards were almost always present at the point of transaction. Identity theft was largely unheard of and chargebacks were rare.

But since then the retail environment has changed beyond recognition. Card-not-present (CNP) fraud has become a huge challenge for online retail.

And with chargebacks, the fraud doesn’t even have to be intentional. Sometimes a chargeback is a deliberate attempt at cyber shoplifting, but often it is the result of misunderstanding rather than mischief.

Customers may have made a purchase in error, or believe an item has not been delivered when it has. In a society primed for instant gratification, the system gives customers a one-click way of asking for a refund, with almost no questions asked.

Data is the answer

The result is that chargebacks on ecommerce transactions are growing faster than the transactions themselves. So what can merchants do? Eaton says the best defence is data.

“At Chargebacks911 we help automate the way merchants and financial institutions collect, compile and interpret chargeback data,” she continues. “We can alert merchants to some potential chargebacks before they happen, letting them stop them at source. And if they do happen, merchants have the information they need to contest an illegitimate chargeback.”

Data might include shipping confirmation numbers, receipt signatures and other evidence. Automation allows the collection and collation of data at scale. Analytics pick up patterns that help identify and then reduce fraudulent claims.

When you have a chargeback data management system, you have the firm foundation for a defence against friendly and unfriendly fraud. Chargebacks911 has helped thousands of companies recover millions of pounds.

“You can only do that with good data,” says Eaton. “As an industry pioneer, we know how to get it and how to interpret it. That saves our customers a lot of money.”

75%

of ecommerce businesses saw an increase in fraud attempts in 2021, with chargeback fraud and misuse now reported to be the top source of fraud affecting merchants

up to

80%

of all ecommerce fraud losses can be linked to chargebacks

Source, 2020

REGULATION

Why 2023 could prove to be a pivotal year for anti-fraud regulation

Legal experts are expecting the enactment of key reforms and new measures, particularly in the economic crime and corporate transparency bill. What might these all mean for UK plc?

Jonathan Weinberg

This year is set to be a significant one for the legislative side of the fight against financial crime in the UK. That means there's plenty of debate about it – in Parliament, boardrooms and legal chambers.

Matt Horne worked for the National Crime Agency for nearly a decade, latterly as deputy director of investigations, before becoming head of policing at government at Clue Software at the end of 2022. He says that, while the legislation is rarely perfect, it remains a key weapon.

"Developments in technology, increasing connectivity and gaps in control are combining to drive the evolution of economic crime. There is an opportunity to turn the tide on this national security threat – and the time is now," Horne declares.

Firms concerned about ensuring their ongoing compliance with the law in this area would be well advised to keep tabs on the likely developments. Here's what they can reasonably expect to see this year.

The economic crime and corporate transparency bill

The ECCT bill went through the Commons in four months and has had its second reading in the Lords. It has two much-discussed provisions, the first of which is the creation of a specific offence covering the "failure to prevent" an economic crime.

Emma Radmore, legal director at law firm Womble Bond Dickinson, says that it's a long-awaited measure.

"Finally, we're getting an offence of failure to prevent fraud and false accounting for all UK businesses (an offence that companies commit when a senior manager is involved) and, for those subject to anti-money-laundering supervision, failure to prevent money-laundering," she says. "Firms should already have policies to prevent the facilitation of bribery and tax evasion. This new offence will broaden their need for risk assessments, top-level commitment and practical implementation."

> We're getting an offence of failure to prevent fraud and false accounting for all UK businesses

184,000

new businesses were registered with Companies House in the third quarter of last year

From 2021 to 2022, the number of new incorporations increased by **2.7%**

5 million businesses are now registered with Companies House

Companies House, 2023

Radmore is referring to the Bribery Act 2010 and the Criminal Finances Act 2017, both of which already apply the "failure to prevent" model. But this has had limited success in securing convictions so far, because a person must hold a senior position in a firm and be able to act autonomously to be held liable under these acts. The new "failure to prevent" provisions in the ECCT bill could make it easier to bring wrongdoers to justice.

At present, the lack of specific legislation on corporate criminal liability in the areas of false accounting, fraud and money-laundering means that proof is required that someone involved in such crimes is a "directing mind and will" of their organisation. The final version of the ECCT bill, on the other hand, is expected to specify that a company's "associated persons" – encompassing employees, agents and other intermediaries – are included when it comes to establishing liability.

This expansion of scope may sound alarming, but employers shouldn't panic, according to Alun Milford, a partner in the criminal litigation team at Kingsley Napley. He says that companies with reasonable prevention procedures in place would not be expected to police every action taken by their employees.

"Firms that operate ethically, understand where their risks lie and take proportionate steps to address these through appropriate compliance procedures should have nothing to fear," Milford explains.

But Francesca Titus, a barrister and partner at McGuireWoods, envisages another potential problem for firms.

"If this offence becomes law, companies will spend millions trying to show that they did all they could to prevent those they do business with from committing financial crimes," she predicts. "The trouble is, the law won't discriminate on the size of company involved. It will hit all organisations, not just those that the Serious Fraud Office wants to target."

Reforms to Companies House

The second ECCT bill provision that's prompted much debate centres on procedures at Companies House. The bill incorporates measures designed to prevent fraud and money-laundering by requiring more detailed information in applications for company registration.

Ivan Heard, global head of fraud solutions at software firm Quantexa, observes that the UK's relatively frictionless process of company formation applies "little to no scrutiny" on applications and those making them.

"The bill should give Companies House the mandate to proactively verify individuals when they register, helping to prevent bad organisations from gaining access to the system," Heard says.

More transatlantic co-operation

Signed last year, the US-UK data access agreement (DAA) requires both countries to ensure that their laws permit a telco in one jurisdiction to respond to direct requests for information made by a relevant authority in the other. It was designed with fighting transnational organised crime, terrorism and child exploitation in mind, but Helen Simm, a partner at law firm Browne Jacobson, points out that it can also be invoked in fraud investigations.

She adds that the DAA raises some concerns about the data privacy rights of technology users: "Companies will need to assess whether there's a legal basis for sharing the requested personal data. This may prove challenging for many, particularly while the provisions are new and have yet to be tested in court."

A stronger grip on crypto assets

Westminster's plans for taming the crypto sector may prove the most significant legislative development this year. That's the view of Indraneel Basu Majumdar, senior financial services solicitor at Harper James.

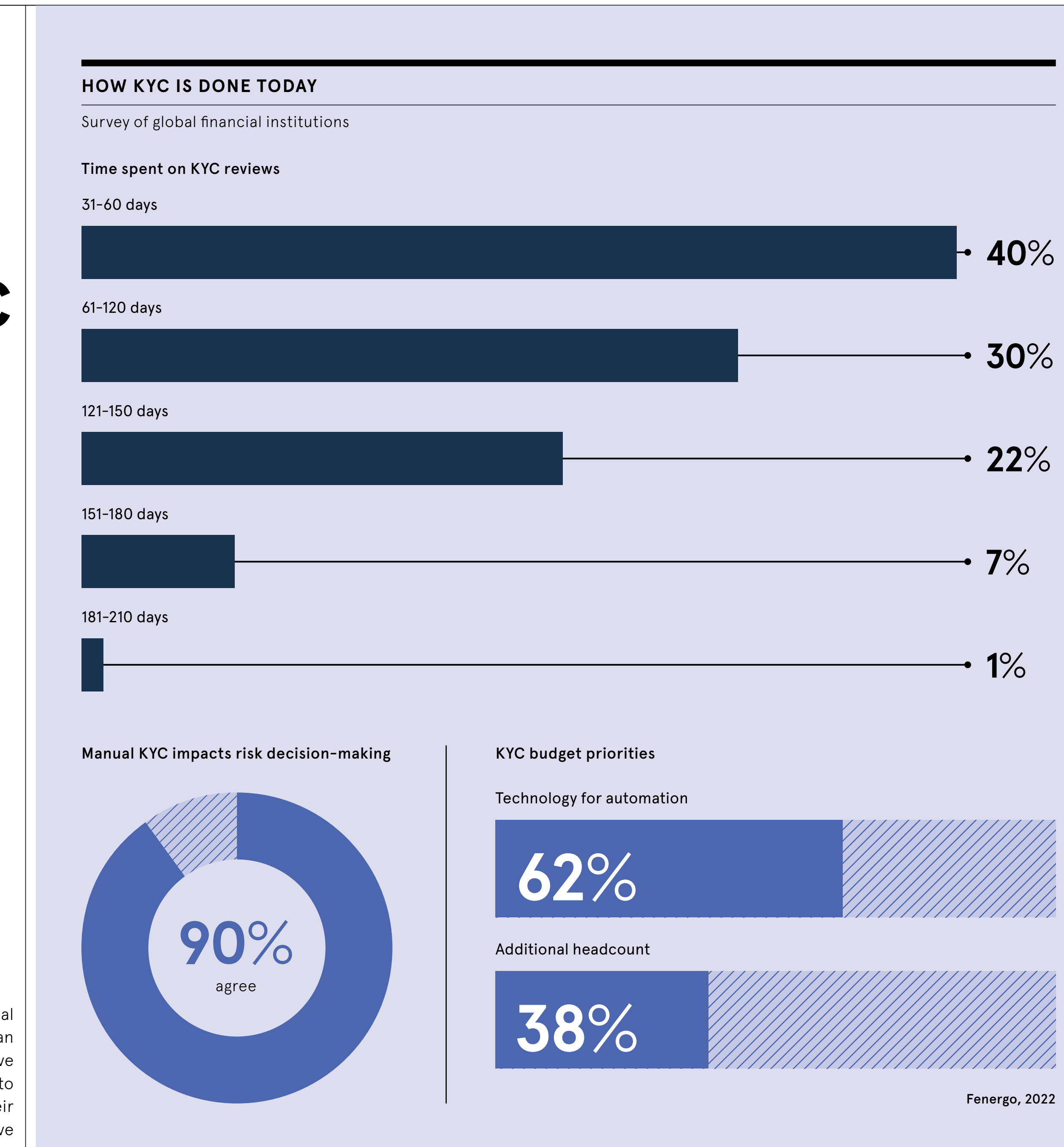
The imposition of new rules could "profoundly affect" businesses in the sector, bringing them within the regulatory framework governing other financial products – and, potentially, allowing crypto assets to "flourish as a valid asset class", he predicts.

For now, though, it's a case of softly-softly. "The phased regulatory approach will enable firms to assess where their businesses will be: within or without the regulatory framework," Basu Majumdar says. "This is helpful for those looking to establish crypto businesses but are worried about the direction of travel."

Commercial feature

Why a dynamic approach to KYC and AML pays

Having a comprehensive view of customer profiles can help to head off issues caused by future changes to regulation



Things have always moved quickly in financial services. But the same is now true of lots of sectors too, especially over the past couple of years. "The world is moving much more permanently online, post-Covid," says Stella Clarke, chief strategy officer at financial software company Fenergo. "Things that we never thought we'd be able to do in financial services, we can now actually do online."

And at the same time, we're facing geopolitical and economic uncertainty on a scale we haven't seen for decades. It all means that investment in new business is tightening, and at a consumer level, people are shopping around for services in a way they haven't previously. It's a buyer's market, rather than a seller's one.

Unfortunately, those customers aren't always being honest in ways they used to. The cost-of-living crisis means that financial crime and money-laundering are increasing as people are tempted to try and one-up the system. And those who aren't deliberately engaging in fraud are often caught up in it as victims. "In an economic crisis, people become much more vulnerable to being defrauded, especially those who are economically stressed," says Clarke.

That creates a double whammy for banks and fintech firms. They're being asked to keep track of ever more elusive customers, doing so remotely thanks to the great post-pandemic move online, while also fearing that ever more stringent regulation could result in enforcement action against them, hitting at a time when they really can't afford to be hauled over the coals.

These macroeconomic and societal trends make it more important than ever for financial institutions to have an automated system and process to onboard customers and check their bona fides. Traditionally, banks have lagged behind other industries when it comes to digital transformation. Many are still stuck in the era of manual checks for compliance, document scanning and signing, and other kinds of paperwork. It's inefficient and off-putting for customers, who increasingly value convenience first. The more time a customer spends becoming, rather than being, a customer, the less likely they are to recommend a service to their friends and colleagues. And a Fenergo survey of chief operations officers, chief compliance officers and chief risk officers shows that 60% of know your customer (KYC) checks take more than 60 days to complete for large corporate customers.

But it's not just the threat of losing customers that's making banks think twice about the old ways of doing things. Nine out of 10 of those surveyed agree that manual KYC processes affect their ability to make better risk decisions. And the more humans are involved, the greater the chance of error.

A manual KYC and customer acquisition process can very quickly become a risk. "Manual checks prevent organisations having a single view of each client," says Clarke. "You can miss tell-tale signs of risk when onboarding is done manually, such as who a company's shareholders are and who they're connected to." That's a reputational and regulatory risk for financial businesses, who say between a third and half of all KYC review tasks are still done manually.

> You can miss tell-tale signs of risk when onboarding is done manually, such as who a company's shareholders are and who they're connected to

It's made all the more challenging by rising competition in the sector, and the need to drive down costs versus your peers. "Banks are facing this increased risk on one side from a financial perspective, but are also being told by their boards that they need to cut budgets or find a better way to solve this problem," says Clarke.

There is a way. Technology can automatically monitor and conduct anti-money-laundering (AML) and KYC checks to ensure financial firms stay on the right side of their compliance requirements, while also making customers happier about the process of banking with them. In total, 62% of executives surveyed by Fenergo say that technology for automation is their key KYC budget priority, compared with the 38% who are looking to increase headcount to make the manual, human-led process more efficient.

For those taking the technological route, it's all about finding the right vendor. "This is what we strive to do. We collect all the information needed from a prospective customer when they want to sign up, whether that's for a business bank account, a big corporate bank account or a high-net-worth individual," says Fenergo's Clarke.

Automating the key processes required to meet regulatory compliance requirements also helps to provide the best experience to the customer. "We're efficient at concentrating on letting the good people come into a financial institution, whether they're a company or a person, but taking care of all the compliance bits that need to happen automatically in the background," says Clarke. This provides a valid, detailed, single client view in real time, helping to mitigate and prevent the risks of money-laundering. It gives the agility and benefits of the cloud, with all the assurance of a data-led approach.

Banks need a solution that provides confidence that they're doing the right thing, even in the fast-moving world of financial regulatory changes. And, even better, this has the halo effect of making customers more confident in a bank's ability to serve them in the best possible way.

Client lifecycle management (CLM) technology of this kind helps banking incumbents move from manual oversight to automated, hands-off checking in real time, ensuring they can keep their position in the market. And for new, nimbler fintechs, it's a chance to get into the market without the large headcount traditionally associated with KYC and AML checks, so they can compete at a high level.

"Whether you have 1,000 people with pens and paper or you use the latest cutting-edge technology, if you don't do it properly, you will be vulnerable to error and you will get fined by the regulators," says Clarke. "CLM technology can solve a regulatory compliance problem and keep out of the way of the customer experience."

And crucially, this is an opportunity for business leaders to focus on generating and growing revenue for the future. "The faster institutions are going to win," says Clarke. "Because they make things easier for their customers."

Sam Bankman-Fried, the founder of FTX, has been indicted on 12 charges and faces a lengthy jail term if convicted

Bloomberg / Contributor via Getty Images

CRYPTOCURRENCIES

Crypto collapso: why fraudsters prosper in a distressed market

Criminals are treating the implosion of the FTX exchange and the declining value of several popular cryptocurrencies as a chance to target a whole new set of potential victims

Sean Hargrave

The demise of a cryptocurrency exchange offers a useful case study of the vicious cycles that can arise in online fraud. When a large exchange collapses, bad actors seeking to recoup their own losses suddenly have many new potential victims in the same boat, whom they can offer 'help' to rescue their accounts.

The most recent case in point is that of FTX, which filed for bankruptcy protection in November 2022 with $8bn (£6.7bn) of investors' money missing and over $400m identified as having been extracted by hackers. While its founder, Sam Bankman-Fried, has pleaded not guilty to charges of fraud and other crimes, this is merely the latest in a string of cases where a combination of reckless mismanagement, deliberate fraud and inadequate regulation has cost unwary investors dearly.

Indeed, the problems extend well beyond FTX. A report published by the Federal Trade Commission in June 2022 estimated that losses to crypto fraud in the US since the start of 2021 had topped $1bn.

Prudent investors might presume that such cases would deter all but the foolhardiest from taking big risks in the crypto markets, leading to a natural decline in fraud. But experts such as Lewis Duke, a senior specialist in SecOps risk and threat intelligence at cybersecurity software firm Trend Micro, disagree.

He predicts an upsurge in crypto fraud in the short to medium term because both criminals and honest investors alike will be highly motivated to chase losses caused by the FTX debacle. Its impact is also putting downward pressure on the values of the main cryptocurrencies, which are already worth far less than they were a year ago. One bitcoin, for instance, was trading at around the $44,000 mark at the start of March 2022. As this report goes to press, it's worth about $24,800.

"The fraudsters will exploit uncertainty and target those trying to recover lost investments through fake exchanges and scams involving initial coin offerings," Duke says. "For the threat actors, there is the extra motivation of the reduced monetary value of the digital currency, as well as the potential for large financial losses should an exchange or currency go offline."

Daniel Seely, an associate specialising in crypto matters at law firm Freeths, agrees. He explains that, while there's always a certain level of fraud in this field, it tends to rise when an exchange fails, because it offers criminals an extra way to swindle distressed investors.

"Once a site is known to have gone down – even temporarily – fraudsters will take it as an opportunity to impersonate its staff and contact affected customers," he says. "They'll often approach victims with an offer to help 'resolve problems with their account', which they claim arose from the outage, and use this as a pretext to obtain information such as passwords, encryption codes and other sensitive data."

> Once a site is known to have gone down – even temporarily – fraudsters will take it as an opportunity to impersonate its staff

One potential silver lining from the FTX scandal and its predecessors is that legitimate exchanges are collaborating more proactively with investigators trying to recover users' funds. That's the view of Josh Chinn, co-founder and director of Wealth Recovery Solicitors.

Getting help used to be a long and costly process for fraud victims, but the exchanges – acutely aware of their sector's Wild West image – have become more willing to offer assistance, he explains.

"Since the FTX scandal, we've seen a huge shift in the way exchanges and end points deal with us," Chinn reports. "In the past, end points usually wouldn't cooperate until our clients had incurred fees to obtain court orders requiring them to do so. Exchanges are being more cooperative, providing disclosures and helping us to work towards recovering lost assets."

The other positive development concerns regulation. The UK's proposed regulatory framework for crypto providers is particularly rigorous. The FTX case is almost certain to build support for this more stringent set of rules to be enacted as quickly as possible.

Andrew Parsons, a partner at law firm Womble Bond Dickinson, believes that the UK could emerge as a leader in legitimate cryptocurrency transactions as a result. Obtaining a registration with the Financial Conduct Authority (FCA), which oversees the UK's anti-money-laundering rules, represents a high regulatory hurdle for crypto providers to clear. Their reward for doing so could be winning the business of the many prudent investors who don't deal with unregulated entities, he says.

"Getting authorised by FCA is a long and complex process, while compliance is always burdensome," Parsons says. "As more unregulated exchanges collapse, it's possible that more people may see the benefits of regulating them in the way the UK is proposing. There are definitely opportunities for exchanges that are willing to commit a lot of resources to securing FCA authorisation."

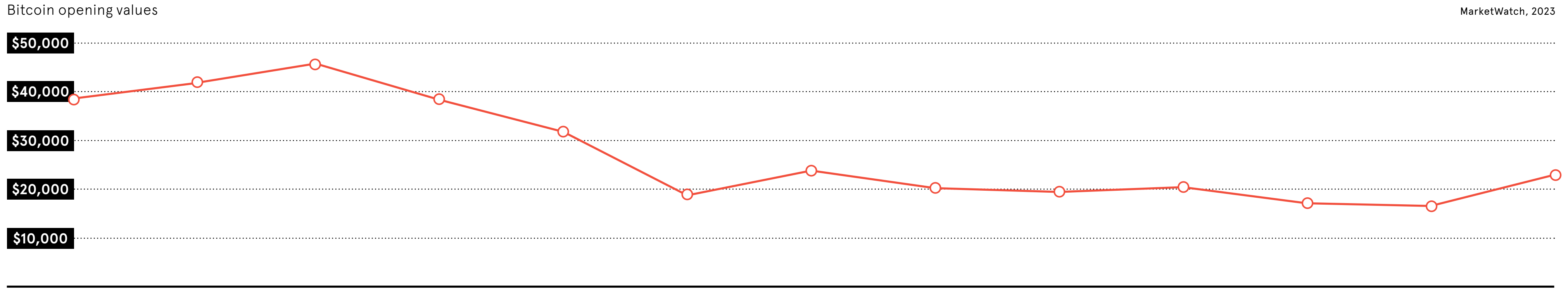
That does not improve matters much in the short to medium term, of course. Neither does the new level of cooperation with investigators, which applies only once an investor has been conned.

Sadly, then, the experts' warnings are likely to be accurate. The criminals are using this particularly turbulent period in the crypto markets to redouble their efforts to defraud people who've already lost out and are in a vulnerable state. The best advice for those distressed investors, therefore, may well be: trust no one – least of all the 'helping hand' who arrives out of the blue offering to recover their money.

THE VALUE OF THE BIGGEST CRYPTOCURRENCY, BITCOIN, SLUMPED IN 2022

Bitcoin opening values

MarketWatch, 2023



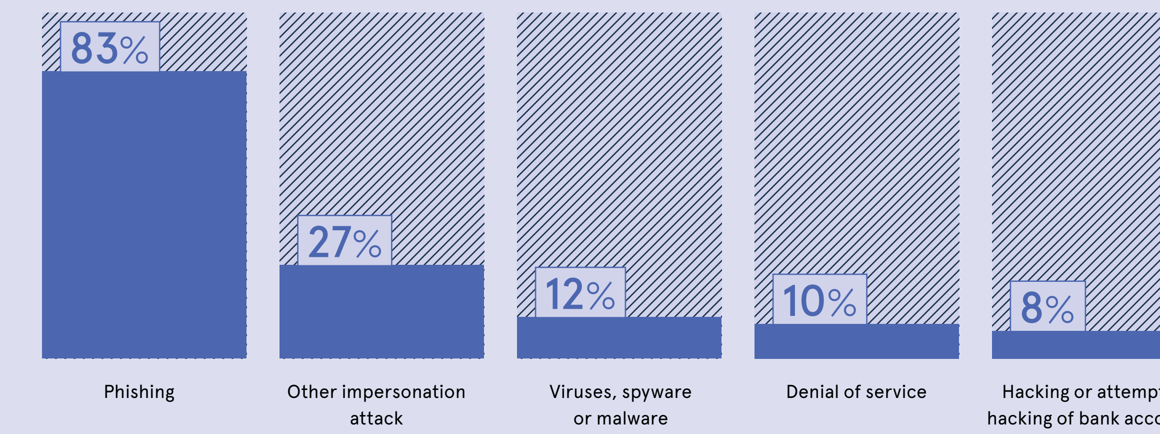
Commercial feature

Targeting the top: how cybercriminals are getting personal

From exploiting digital footprints to weaponising advanced AI, online fraudsters are expanding their toolkit. Is it time for senior executives to watch their step?

HOOK LINE AND SINKER: THE PHISHING THREAT TO BUSINESS LEADERS

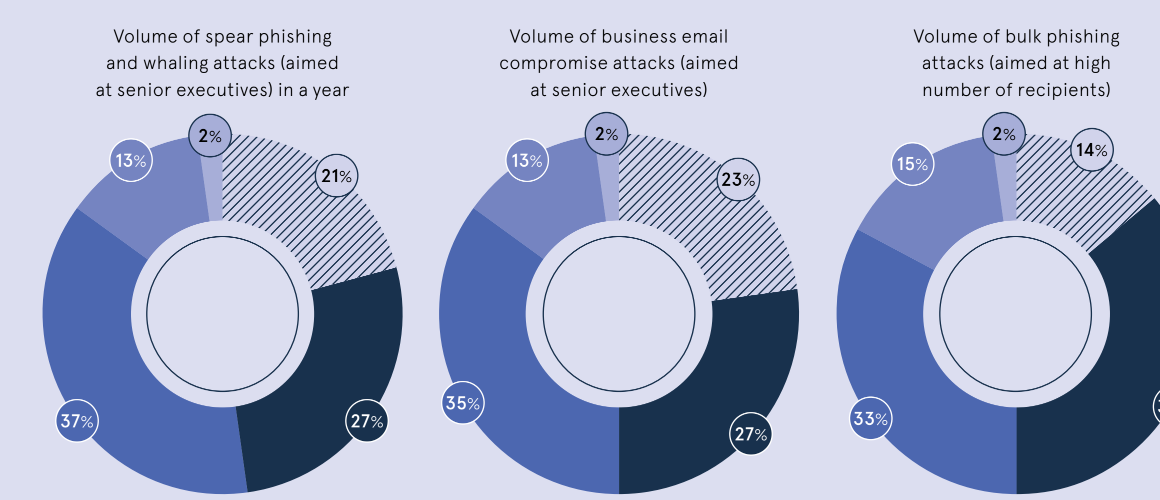
When UK companies experience cyber attacks, what is the nature of the threat?



50% of attacked companies said phishing and impersonation attacks were most disruptive

gov.uk, 2022

Cybercriminals are directly targeting the C-suite



Proofpoint, 2022

Although the C-suite can be a tough nut to crack, the potential payouts from a successful whaling attack – one that targets top-level executives – can make cracking it well worth a fraudster's time.

In a world where almost everyone has a digital presence, cybercriminals have all the resources at their disposal to get to know their mark – and the ramifications can be devastating for senior executives caught in the crosshairs.

According to the UK government's Cyber Security Breaches Survey, phishing constitutes the most common cyber threat vector for businesses, with 83% of the organisations that spotted attacks registering this as the scammer's chosen method. And with the wealth of information that is shared publicly across various online spaces, whaling attacks are becoming a serious cause for concern.

Kraig Rutland, VP for cyber security at Aon's Cyber Solutions, explains: "A lot of the time, senior executives have an important public profile and digital presence. The evolution of an individual's digital footprint has accelerated rapidly over the last decade with social media, online platforms and content – not just personal but professionally too."

The motivation behind tactical whaling attacks is almost always financial, but the fallout can be reputationally and legally devastating. In one well-publicised instance, an Austrian aerospace manufacturer lost €50m from a targeted email attack which resulted in the firing of several employees, including the company's CEO.

And possibly the most nefarious aspect of such whaling attacks is how attackers gain access. Frequently, they exploit information in the public domain – social media posts from friends and family, their hobbies and interests, or their location.

"They're targeting down. One organisation in the States was the victim of a massive ransomware attack," says Kate Kuehn, chief trust officer at Aon. "When they did the forensics, they found out they got in through the CEO's wife's phone. He'd borrowed it and sent a few things over text when it was compromised. The attack put the company out of business," she says. "The line between public and private is so blurred."

Other more deeply personal profiles can also be a source of rich data – but also potential embarrassment. "The information on elite dating sites is an area where attackers can manipulate data, and it's exactly the sort of place you'd expect to find high-net-worth individuals," says Kuehn.

These sites, among others, lay out an opportunity for criminals to build trust and convince targets to invest larger and larger sums of money from crypto wallets or offshore bank accounts.

The tools that attackers now have in their arsenal provide an acute ability to replicate the sort of communications senior executives expect to see in their inboxes, eliminating many of the usual red flags. AI chatbot services, like ChatGPT, Bard and Claude, to name a few can be misused and become a fraudster's friend, making it even easier to deliver fast, effective, frequent attacks. Advanced natural language tools can even offer scammers from outside the English-speaking world new levels of natural language fluency in their communications.

And the expanding use of AI makes it likely that there will be far more sophisticated social engineering attacks in the future as it becomes challenging to distinguish between genuine and fraudulent communications. Some tools can detect the use of AI, but these are still playing catch-up while deepfake technologies and AI chatbots get more sophisticated.

Rutland believes that recognising the risks posed to individual executives alongside the fundamental cyber threats facing organisations is an important measure. "We have to go back to understanding the risks and find new ways to mitigate them as the landscape continues to evolve," he says. "Executives will need to be more conscious than ever about the information they put out there. When they get an email that might seem like an obvious request, consider a self-check built into the system: Am I expecting this? Should I be responding? How did that information get in there, and is there a way to validate this?"

The assortment of vulnerabilities hackers can exploit, from family and friends to associates, can see businesses engaging in a high-stakes game of whack-a-mole. But there are ways to plug the gaps.

Assessment is the first port of call. It's vital to understand the threats you are most vulnerable to and what you can do to better protect yourself against them. Senior executives can start by understanding their own level of exposure. Aon delivers tailored individual vulnerability assessments, or IVAs, as part of its cyber loop risk management model.

This gives executives visibility over threat exposures. They can then use this data to drive the decision-making required to manage their own digital footprint. A similar approach can be taken for their organisations. A comprehensive cyber risk assessment can be performed to determine risks, threats and financial exposures, which in turn helps businesses to prioritise mitigation measures and budgets to better maximise cyber resilience.

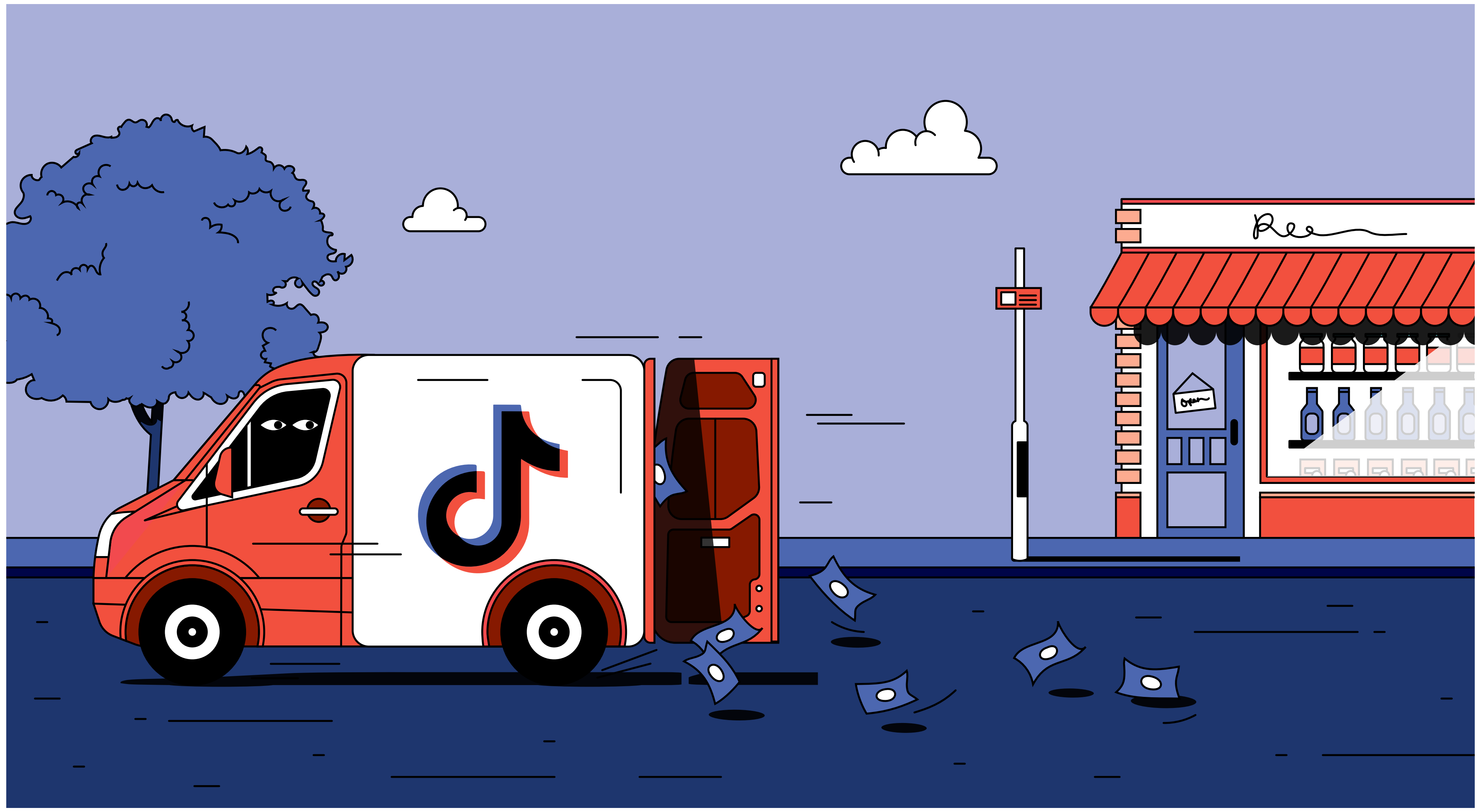
It's vital to be comprehensive in assessing risk, according to Rutland. "There is a business risk, operational risk, financial risk, reputational risk, and even supply chain risk. Cyber now lives in all those towers, so an organisation must constantly be assessing and understanding its cyber maturity and using this insight to make data-driven decisions on how to manage accordingly," he says.

Aon's cyber loop model for sustained cyber resilience identifies four entry points. Rutland explains: "These points aren't linear, and organisations can enter at any stage: you may enter at a time of recovery, or financial transfer, for example, which leads to further need to assess cyber risk. Mitigation is understanding where there might be a control gap and closing it through people, processes or technology," he explains. "You can move from assessment to transfer or recovery to mitigation or any number of combinations. What is important is that managing cyber risk is not a single point in time activity. It is a circular process and needs to be continuously reviewed."

> Managing cyber risk is not a single-point-in-time activity. It is a circular process and needs to be continuously reviewed

The sheer number of ways organisations and individuals can be exposed to cyber risks might seem daunting, but it needn't be despairing. Businesses can establish a culture of vigilance and preparedness that puts them on the path to sustained cyber resilience.

"It has to be in constant deployment all the time," says Kuehn. "Cyber is always changing. It's a never-ending journey, and there's always going to be innovation that we have to think about."



SOCIAL MEDIA

Bad influencers – the rise of TikTok fraud

The video-sharing platform's built-in virality means that information about any opportunity – legal or otherwise – for hard-pressed consumers to get one over on big business will spread far and wide

Chris Stokel-Walker

Tesco started to notice that something was wrong last summer when its confectionery shelves were being emptied at an unprecedented rate. Shoppers were coming into its supermarkets across the UK and clearing out their stocks of Fruit Pastilles, M&M's, Maltesers, Skittles and Starbursts.

It took a little while for the management to understand what was happening. It turned out that people were exploiting a glitch in the self-checkout software, which had been exposed by the £1 discount vouchers that Tesco had issued for certain sweets. These were meant to be single-use coupons, but in practice they could be applied several times – as shoppers had so quickly realised.

When such things happen, social networks enable the word to spread like wildfire. TikTok was the main conduit in this case. The so-called Tesco method, which one TikTok user called "the biggest coupon fraud scam that's ever hit the UK", became the focus of hundreds of clips on the video-sharing platform. Smartphone-toting shoppers shared footage of themselves walking out of stores fully laden with free sweets, encouraging more copycats in the process. Tesco responded by posting warning signs at its checkouts threatening to prosecute anyone trying the same trick.

The Tesco method is far from the only Robin Hood-style scam that has spread via TikTok. In recent cases, users in the US have highlighted ways to obtain bank loans for personal use by setting up a fake business and to commit leasing fraud by providing fake documents.

Such methods are typically presented as simple money-making exercises – ways to outsmart businesses that have been lax enough to leave loopholes – rather than offences involving deception.

"These obviously aren't 'finance hacks'. They are crimes," says Carl Wearn, head of threat intelligence analysis at Mimecast. "The individuals using them are clearly, and often knowingly, exploiting what they perceive to be flaws in an offer – Tesco's vouchers, for instance – and are in essence committing fraud to obtain property."

Even so, the sharing of fraudulent methods, including advice on how to obtain and use stolen credit card information, is catching on quickly. The #methods hashtag, under which such tips are traded, has become particularly popular with an impressionable demographic in the UK over the past six months. It's estimated that almost 90% of those watching #methods videos are aged between 18 and 24.

Some clips are posted instead under the #financialliteracy hashtag, which has attracted 1.2 billion views on the app. These have included videos suggesting that you don't necessarily have to pay your bills under US consumer law. Such hacks are typically presented as personal success stories, along with the implicit message that everyone is already doing it. This aspirational aspect is another part of what makes such material so dangerous, observes Gavin Cunningham, partner and head of forensic services at accounting firm Menzies.

"Two decades ago, no one would have taken, say, tax advice from a flyer that had been posted through their door," he says. "Because such information is instantly available, people tend to believe that it's real, accurate and honest."

Other videos that have proved popular on TikTok have been uploaded by users professing to have bought two pairs of trainers – an authentic pair from a shop and a cheap counterfeit copy online – and then returned the fakes to the shop for a refund while keeping the genuine ones. Another suggests that people can somehow reduce their tax liability by buying a car on credit and then selling it after depreciating its value on their return.

And it's not only financial scams that TikTok is helping to promulgate. Other forms of deception are being normalised on the platform, including the idea that it's acceptable for job applicants to lie about their experience on their CVs. One woman went viral for saying that she routinely searched YouTube for guidance on how to do her job because she had overstated her qualifications during her employer's selection process and couldn't perform the tasks assigned to her.

It should come as no surprise that, just like any other digital watercooler, TikTok has become a place where people trade tips on how to get one over on big business.

"TikTok's culture of scamming is proving exceedingly lucrative and effortless," says Tom Divon, a researcher at the Hebrew University of Jerusalem specialising in social media, communications and culture. "This phenomenon can be attributed partly to the ease with which one can adopt a fraudulent persona on the platform."

> **TikTok's culture of scamming is proving exceedingly lucrative and effortless**

There's also a degree of fame to be had by sharing such tips, especially in an inflationary period when consumers are more likely to feel that they're getting ripped off by profit-hungry corporations.

"TikTok is home to a diverse range of influencers who are reputed to possess knowledge of various legal and financial hacks," Divon says. "They've earned social capital by showcasing an altruistic approach in their videos that appeals to the communal sensitivities of viewers who feel burdened by the 'robbery culture'," he says.

This is, naturally, a trend that TikTok is keen to quell. It says: "As more people seek financial information online, it's important that we help our community to access the right support and tips. We have strict community guidelines, which make it clear that we do not permit anyone to exploit our platform to bring about financial or personal harm. We remove content and accounts that violate these policies."

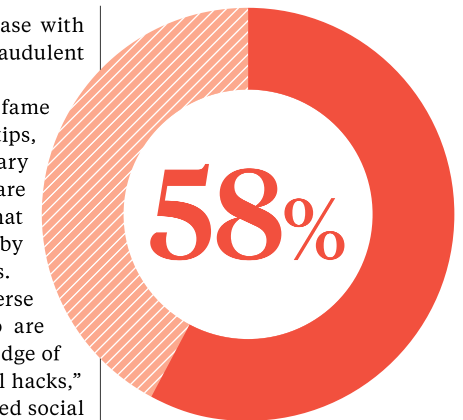
The platform adds that it has partnered with the Citizens Advice service and recently launched a #savingmoney hub offering legitimate financial tips for consumers.

Nonetheless, while millions of households struggle to make ends meet as the cost-of-living crisis continues, any money-saving tip – whatever its legality – will hold some appeal to cash-strapped social media users.

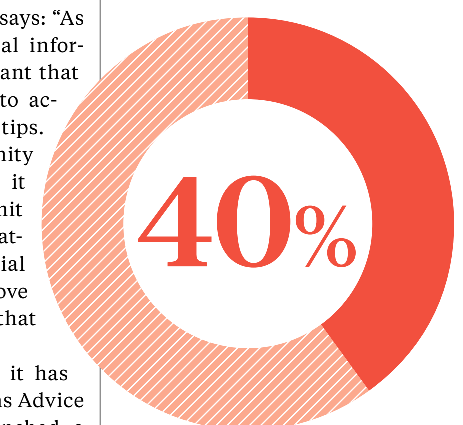
For that reason, firms may want to monitor TikTok to keep an eye out for any conversations mentioning their name. It can be useful to search for posts featuring the hashtags typically used to promote these kinds of scams.

Another way to combat viral fraud, of course, is to prevent it by ensuring that your systems aren't left vulnerable to simple hacks in the first place.

"Brands are often keen to exploit electronic means of redemption precisely because these are quick and easy to use for discounts," Wearn says. "But, in my experience, they rarely put the appropriate measures in place to properly mitigate the exploitation of such schemes by human ingenuity. As long as organisations use half-measures when it comes to security, the issue will persist." ●



of 18- to 24-year-olds follow TikTok influencers who talk about personal finance



of these users say that influencers give them better financial advice than that delivered via traditional media

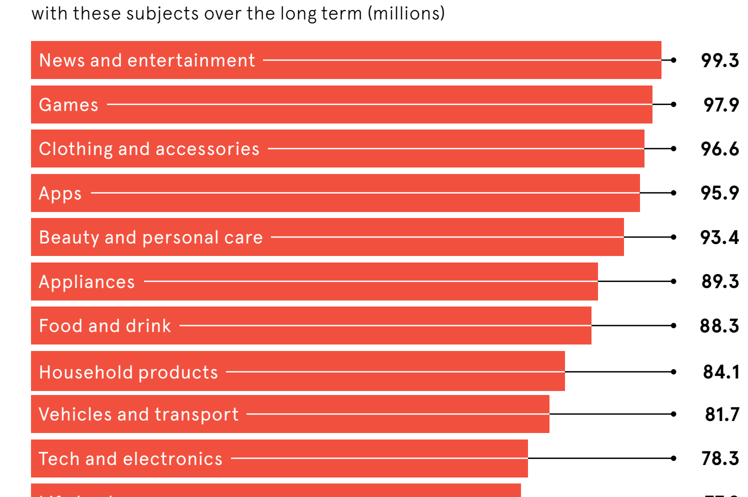
1/2

have made financial decisions based on social media content

Current Account Switch Service, 2022

FRAUDULENT ACTS, MASQUERADING AS 'HACKS', HAVE BEEN RECOMMENDED TO MILLIONS OF TIKTOK VIEWERS WORLDWIDE

The most popular user interests on TikTok, by the number of accounts engaging with these subjects over the long term (millions)



Socialinsider, 2022