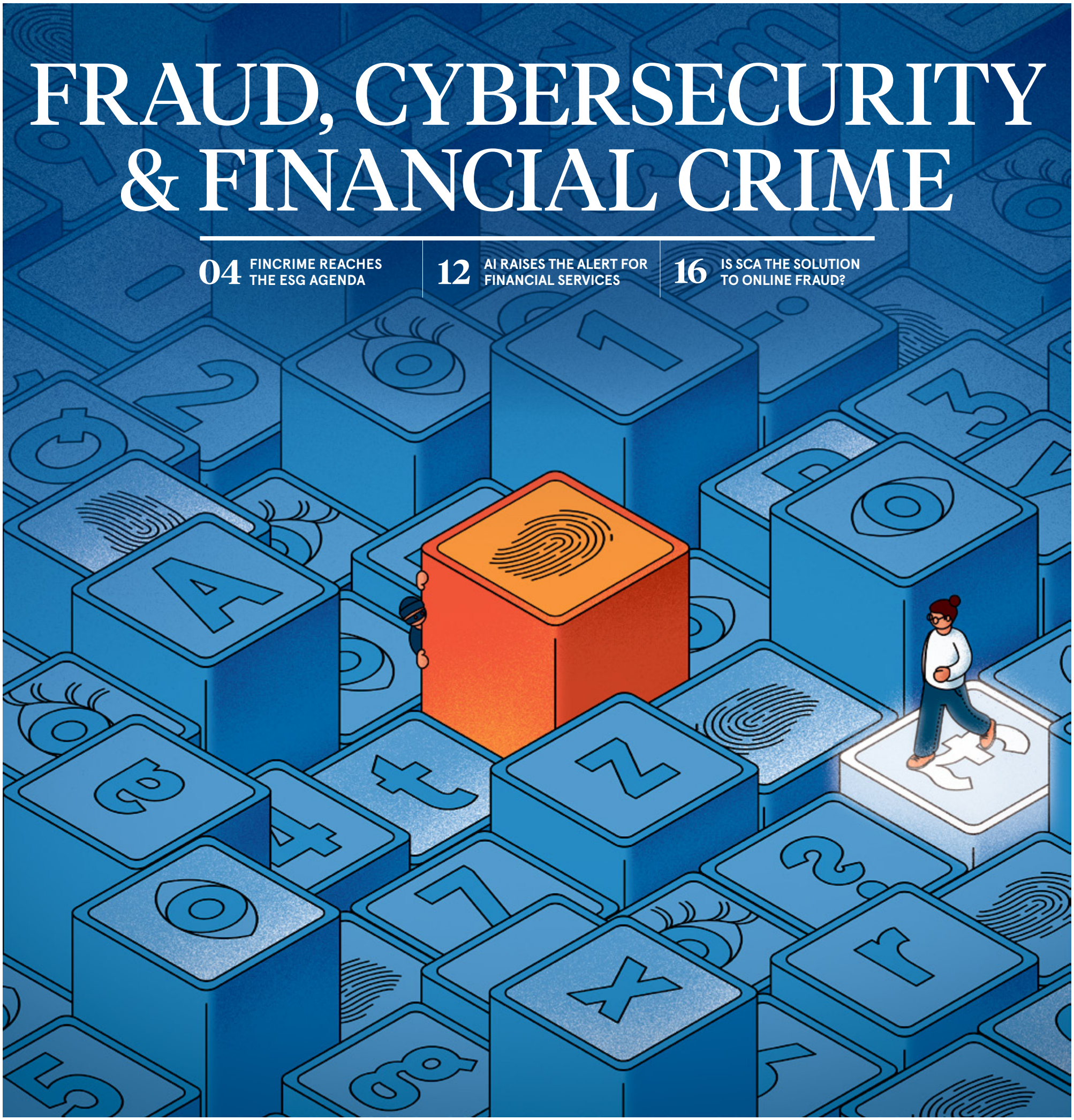
FRAUD, CYBERSECURITY & FINANCIAL CRIME



FRAUD, CYBERSECURITY & FINANCIAL CRIME

Distributed in THE TIMES

Published in association with cifas
The UK's Fraud Prevention Community

Contributors

Diana Bentley
A former lawyer, now writer with over two decades of experience covering law, finance, business, culture and travel.

Tim Cooper
An award-winning freelance journalist with 20 years' experience. He has written for many publications, including *The Spectator, The Guardian* and *The Telegraph*.

Sean Hargrave
Former *Sunday Times* innovation editor, who is now a freelance journalist covering technology, business issues, financial services and digital marketing.

Oliver Pickup
Multi-award-winning journalist specialising in business, technology, sport and culture.

Simon Brooke
A freelance journalist with 25 years' experience of covering business and finance, wealth management, sustainability, the luxury sector, and marketing and communications for a wide variety of outlets.

Ben Edwards
A freelance journalist specialising in finance, business, law and technology, with more than a decade of editorial and commercial writing experience.

Joy Persaud
Journalist, biographer and author writing on subjects including business, health, diversity and education for the national press and blue chip companies.

Chris Stokel-Walker
Technology and culture journalist and author, writing for *The New York Times* and *The Guardian*.

raconteur reports

Publishing manager
Narinder Hayer

Managing editor
Sarah Vizard

Deputy editor
Francesca Cassidy

Reports editor
Ian Deering

Sub-editors
Neil Cole
Christina Ryder

Commercial content editors
Laura Bithell
Brittany Golob

Head of production
Justyna O'Connell

Design/production assistant
Louis Nassé

Design
Kellie Jerrard
Colm McDermott
Sean Wyatt-Livesley

Illustration
Celina Lucey
Samuele Motta

Design director
Tim Whitlock

@raconteur raconteur-media @raconteur.stories

raconteur.net /fraud-financial-crime-2022

FRAUD DETECTION

The UK's ongoing fight against fraud

Fraud is hitting the UK hard. Why are we failing to tackle one of the biggest threats to our security?

Joy Persaud

The UK is beleaguered by fraud – and the problem shows no signs of abating. The *Annual Fraud Report 2022* by UK Finance, which represents the banking and finance industry, calls for greater cross-sector action to tackle the issue.

Fraudsters are increasingly skilled. They adapt their methods to exploit vulnerabilities and the changes in consumer lifestyles and behaviour since Covid.

A key concern is the rise in the number of impersonation scams and authorised push payment (APP) fraud. This is when a payer is deceived or defrauded into authorising a payment to a criminal. UK Finance members reported 195,996 incidents of APP scams in 2021 with gross losses of £583.2m, compared with £420.7m in 2020. Of the total, £505.8m related to personal losses and £77.4m affected non-personal or business transactions.

It is clear the problem is widespread. Last year, communications regulator Ofcom found that eight out of 10 people surveyed had been targeted with scam texts or phone calls designed to convince them that they were from trusted organisations such as banks, the NHS or government departments.

"Fraud has been the most common form of crime for several years. And the threat continues to evolve and diversify," says Mike Miller, economic crime manager at ICAEW. "Technological advancements and geopolitical shifts provide the backdrop for nefarious actors – be they nation states, organised criminal groups or petty criminals – to diversify their targets and methods of attack.

"Mobile technology makes it easier for criminals to target victims directly, through various communication methods. And the government's Covid financial support packages have presented more opportunities for fraudulent claims such as for furlough payments."

APP fraud often involves social engineering – scam texts, phone calls and emails. With the move towards buying online, which ramped up necessarily during the pandemic, the opportunities for criminals abound. Fake websites and adverts featuring celebrities have been used by many unscrupulous types to encourage consumers to hand over their personal details – and, of course, their cash.

skaman306 via Getty Images

Peter Taylor is a fraud consultant and former CID fraud officer. He says that fraud has long been embedded in the UK and is habitually dismissed as victimless. But the devastation wreaked by fraudsters should not be underestimated. The crime manipulates human curiosity and our inclination to engage with others; it can damage victims' mental as well as physical health. According to Age UK, older victims who have been scammed are 2.4 times more likely to die or go into a care home than those who have not.

"Criminals are creatures of habit. And if they make money, they will keep coming back," says Taylor. "The disruption from Covid and the funds available accelerated the growth of fraud – so it's hardly surprising we are at the front of the queue of committing and being victims of fraud. We also have large networks of UK-based organised crime groups who have added fraud to their portfolio.

"When we add the fact that there is so much digital access to people in the UK, English being the most spoken language in the world, and a lack of arrests, we are an attractive prospect globally," he says.

Fraud is so rife that the National Crime Agency says it is the most common crime in the UK, costing billions of pounds every year. It's thought the crime is under-reported, so the problem is likely worse than official figures state. As well as the personal losses of vulnerable victims, duped businesses may collapse.

Organisations with a dedicated fraud programme spend up to

42% less on fraud response

and **17%** less on remediation than their peers

PwC, 2022

Stoyan Barrett is a specialist crime operations investigator and cybersecurity expert. Smaller businesses are increasingly interesting targets for attackers; they know that many firms simply don't think they'll be targeted.

"How might you deal with a system lockdown, a ransomware attack, followed by a request for £20,000 to unlock your business? Savvy up: tech is valuable, so let's treat it as such," he warns. "If an SME does not prioritise cybersecurity as a fundamental, then sadly when they fall victim it isn't difficult to see why so many are unable to recover.

"We should now be targeting cybercrime and cybersecurity in much the same manner as smoking, as it represents the largest threat to our economy."

To try to address the problem, UK Finance heads up the Take Five to Stop Fraud campaign to raise awareness and help consumers and businesses to protect themselves. It encourages people to stop and think before parting with money or information; to challenge – stressing that it's fine to reject, refuse or ignore any requests, and to protect – contact your bank immediately if you think you've fallen for a scam.

But while prevention is a common-sense approach, some experts believe there needs to be a single body to combat fraud. The current approach is piecemeal, with dozens of bodies pitching in, and relies on potential victims to be astute.

"Almost all the regulations that we have to tackle fraud are poorly enforced and place the burden of detection on the companies on the front lines. That system would work if oversight by regulators was more than it is currently – largely due to lack of resourcing," says security consultant James Bore.

He thinks that the number of bodies responsible for tackling fraud needs to be simplified. "It's largely no longer a regional issue, so it makes little sense to have regional police authorities responsible for tackling fraud. And beyond that, there are multiple bodies acting on economic crime: centralising these into a single, well-resourced agency with a single purpose would make a world of difference," he says.

It is perhaps a sign of the times that even UK Fraud and the National Crime Agency, among other official organisations, warn website visitors that fraudsters have impersonated them. It makes it yet more difficult to know who to trust.

ANTI-FINANCIAL CRIME

Tackling the G in ESG

Financial crime finally climbs the governance agenda, but offences keep rising

Tim Cooper

It has taken a war to trigger it, but anti-financial crime is finally moving up the governance agenda for companies and investors.

Organisations must already comply with a slew of regulations aiming to identify and prevent financial crimes such as corruption, money laundering and fraud. But until recently, anti-financial crime (AFC) was not a strong part of governance frameworks, say experts. This is despite six of the 36 consensus measures of governance relating directly to financial crime, according to data firm Clarity AI. Consultant Deloitte says companies should also see AFC as part of their ESG strategy because it plays a critical role in stopping heinous crimes such as human trafficking and terrorism.

Tom Keatinge is the founding director of the Centre for Financial Crime and Security Studies at the Royal United Services Institute, the UK's leading defence and security think tank. Financial crime, he says, has not typically been a focus of companies' environmental, social and governance (ESG) departments. The invasion of Ukraine, however, has required them to consider corruption and other financial crime risks more closely in business dealings. "The war has galvanised the government and the ESG community to finally prioritise AFC," he notes.

Arun Chauhan, director at Tenet Compliance & Litigation and committee member on the Fraud Advisory Panel, agrees. "Financial crime has not been high enough on the ESG agenda," he says. "It's in the mix now, but still isn't a priority."

Investors are upping the ante, too. Anneka Randhawa, partner and co-head of the London White Collar team at White & Case, says: "There is a strong incentive to investigate financial crime from existing laws. But pressure is also now coming from the rising interest in ESG, with stakeholders increasingly holding companies to account."

Meanwhile, pressure on companies to fight financial crime proactively – whether as part of ESG strategy or not – has been building. The recent FinCEN and Pandora Papers leaks shone a harsh spotlight on the scale of economic crime in the UK. The Ukraine war and the desire to sanction criminals who support the Russian state added urgency to respond. This led the government to fast track its Economic Crime Act 2022, after what many see as years of political foot-dragging.

During the pandemic, fraud scandals in public procurement and furlough payments increased public awareness of financial crime. Meanwhile, organised crime is growing and enabled by technological developments, according to a PwC report.

There is a financial incentive too. Companies worldwide generally lose 5% of their annual revenues to fraud, according to a survey of certified fraud examiners – but it can be more than 10%. Associated reputational damage can also damage their share prices. Chauhan says that, even if companies can save 1% or 2% by preventing fraud, it is worth the investment.

Sarah Gore Langton is chief compliance officer at financial services firm IG. She says her company has been increasing AFC efforts for the past five years. "We have responded to a growing shift in expectation that firms not only meet regulatory obligations but also take a proactive stance in stopping criminal behaviour at source.

"We see two focus areas. To ensure AFC controls are as holistic as possible and to use data science and other technologies for smarter and quicker analysis of suspicious behaviour." An example of a holistic approach would be to consider the risk of other crimes while assessing bribery risk.

Dan Hartnett is director, third-party risk intelligence, at technology and data company Refinitiv. He notes that companies are also under growing pressure to address financial crime risks in suppliers, due to the increased complexity of supply chains. "This necessitates well-designed due diligence programmes, and increased transparency through risk assessment of third parties," he says.

Ways to increase transparency include making it subject to internal audit, and digitising and centralising due diligence data to ease access. Keatinge says one problem with integrating ESG and AFC activity is that, in most financial institutions, they are in silos – despite both relying on detailed understandings of client activity. Companies could exploit clear synergies by merging these silos, he says. Box-ticking is another problem.

"For too long AFC has been about compliance, rather than disrupting financial crime," he says. "This is changing as banks take an intelligence-led response that delivers results for society, not just regulators." This requires companies to redeploy resources, and regulators to support innovation – which, he says, they are not typically keen to do. "Perhaps regulated institutions should be required to produce an annual financial crime statement detailing activities and procedures. The Modern Slavery Statement transparency requirement has driven up standards in ESG and allowed analysts to compare organisations' approaches. AFC could learn from that," he says.

Chauhan adds that there is lots of best practice guidance freely available from regulators, trade and professional associations, professional firms and other bodies. So companies have no excuse for poor practice.

> **Financial crime has not been high enough on the ESG agenda. It's in the mix now, but still not a priority**

8%

of global organisations which encountered fraud in the last 24 months experienced ESG reporting fraud

PwC, 2022

Dev Odedra, director of Minerva Stratagem Consulting, says proactive human engagement is critical to boosting AFC efforts. Many companies focus so much on following regulations, they lose sight of their goal to detect and prevent wrongdoing.

"Regulation doesn't stop financial crime – you do," he says. "You can know all the laws, but they often don't stop the crime."

This year, Transparency International said repeated efforts to strengthen corporate rules have not improved anti-corruption scores – many Western countries' ratings have fallen. Meanwhile, many banks and supporting firms help criminals maintain illicit networks, said the group.

To stop such crimes, you need a deeper understanding than that required by regulation, says Odedra. "For example, the rules tell you to cross-check against sanctions lists. But if you read the news carefully, you know many currently active criminals are not on any sanctions list – or you might spot other details that help identify a suspicious transaction," he says.

INSIGHT

'In a data breach, comms has a crucial role, but it can often be overlooked in the rush'

Cybersecurity is now, rightly, a board-level consideration, but when a breach happens it's crucial companies don't overlook comms in their response, says **James Carter**, CEO at Touchdown PR

Q How has the evolving threat landscape collided with social media to increase the reputational risks facing companies?

A The risk of a cyber attack is growing every day and you need look no further than the long list of high-profile victims to see that the reputational damage to your brand can be enormous.

There's nowhere to hide – people get their news from everywhere. It's 24/7, it's global and, on social media, news travels faster than it ever did via traditional media.

In fact, its real-time nature means social media is often where companies first identify there has been a breach. It's in the public domain before you can start reacting, making your crisis response much more challenging. You must not only monitor the conversation but also actively engage with it, clarify points and respond on various channels to ensure misinformation doesn't spread.

Q How important is communication when responding to a data breach?

A Comms has a crucial role to play, but it can often be overlooked in the rush to ensure the right regulatory boxes are being ticked. We know fines for data breaches can be significant, but even when a company does all the right things from a compliance standpoint, if you don't communicate effectively with your stakeholders, the reputational damage can be costly too.

This makes it essential that PR has a place at the top table from the minute a breach happens. We might not know the nuances of a cyber attack from a technical perspective, but neither do your customers. What they care about is their data, and we know how to craft messages that resonate with them.

In a breach situation, there's a lot of heat and you need to be able to communicate in clear, unemotional language that your customers will understand. We can translate the technical information into something customers can easily digest while building their confidence that you're doing the right things to protect their data.

Q What are your top comms tips for organisations that have been breached?

A Fundamentally, PR is about building trust between brands and customers, and during a breach that doesn't change. The key is to be open and honest, keeping customers informed along the way.

You'll get a lot of grace for acting quickly, but rushing causes mistakes. It's a fine balance. Take a step back to review what is happening in a calm and considered manner, and then move decisively.

It's also vital to think globally. A US-centric response might not land so well in your other regions. A proper comms plan will ensure you have the tools to disseminate the information in different languages at a local level, so all customers feel like they are being considered.

Q How does Touchdown PR support companies in this area?

A Planning for a crisis enables you to spring into action when one occurs. Identifying the key players and processes, we help our clients create a comprehensive crisis comms plan that works on a global scale.

Then we help stress test the comms plan, as well as constantly ensuring it's up to date. It's crucial everyone buys into it. As a global agency we deliver a 'follow the sun' approach for our clients. This ability to constantly monitor all regions is critical in a crisis. Even if you don't normally work with a PR agency, if you do suffer a breach the value of bouncing ideas off third-party comms leaders who deal with crisis situations day in, day out, can prove invaluable. ●

James Carter
CEO, Touchdown PR


DuckMinyy via iStock

COMPLIANCE

A fine challenge: stay current in fight to tackle financial crime

Organisations must carefully manage their strategies if they are to keep pace with updates to AML law

Diana Bentley

Few regulations are more vital to the financial services sector than those which tackle anti-money laundering (AML). A significant challenge for businesses, however, is that the laws are ever-changing.

"The regulations are frequently updated to address developments in the financial services industry, the new methods criminals employ and the recommendations of international bodies. Although the fundamental aim of the regulations remains consistent, the AML regime is becoming more complex and we can expect the regulations to continue to evolve," says Shaul Brazil, a partner at BCL Solicitors.

Recent amendments to the regulations include the addition of further kinds of activity, such as cryptoasset businesses, the insertion of new high-risk factors to be taken into account when assessing the need for enhanced due diligence and the introduction of a requirement for firms to report discrepancies in beneficial ownership information.

The reach of AML regulations extends from global financial organisations to small startups. All of them, though, must satisfy a wide range of requirements. These include conducting risk assessments and implementing AML procedures such as due diligence on new customers, record-keeping, training, appointing compliance officers and making reports. Constant vigilance is required to satisfy some in particular, such as evaluation of customers (especially those who are high risk), monitoring transactions (including bank deposits), and detecting suspicious activities that might need to be reported to the relevant authorities.

> **The reach of AML regulations extends from global financial organisations to startups. But all of them must satisfy a range of requirements**

Exactly how effective an organisation's AML controls are will depend on its risk profile, says Brazil. "There's no one-size-fits-all and the policies and procedures that firms adopt must be appropriate to the nature, size and risk profile of their business."

Whatever their size, firms should take a holistic view of the purpose of the AML regime to avoid compliance problems, he says. "The FCA has demonstrated in its recent enforcement actions that it is less concerned with the finer details of the AML procedures and more with their fundamental purpose.

"Firms should avoid a tick-box approach. They can fall foul of the regulations, not because they haven't implemented them on paper, but because they haven't focused on their purpose and whether their procedures are operationally effective."

Clear documentation and processes that all staff can access and understand can certainly help, says James Alleyne, legal counsel at Kingsley Napley and formerly of the FCA. As a matter of good practice, he advises, organisations should be proactive and not reactive. "Firms should constantly review and update their AML systems, so they're tailored to the changing regulatory standards and political and market developments."

The risks for firms falling foul of AML regulations are, he warns, daunting. Investigations by the FCA, which supervises AML law compliance in the financial services sector, can be costly, time-consuming and may cause business disruption. While the FCA can provide feedback to firms with inadequate crime systems and controls, it can also impose penalties for past breaches. In the past few months alone, it has imposed some £15.7m in fines on several firms found guilty of regulatory failings.

For many organisations, technology is easing the compliance challenge. Customer due-diligence software is well used by newly established fintech consumer lender Tembo, recently named UK's best mortgage broker and best newcomer at the British Banking Awards. "We're a young, digital-only platform which operates in a relatively high-risk area and with multiple customers. We were warned at the outset that we could be a target for criminal activity," say co-founder and CEO Richard Dana and compliance lead Ellie Riordan. "A key element of compliance for us has been using technology to automatically cross-check customer data and verify customer identity and recognise potentially fraudulent behaviours."

Crucially, commitment from senior management is not only expected by the FCA but is essential to create awareness of financial crime throughout an organisation. "It's important to have a strong team culture and that starts with strong leadership, which sets the tone for compliance," say Dana and Riordan.

"You must ensure that your different teams work together effectively and that compliance is included right at the beginning of any change to operations or product. We have honest, open discussions about compliance and people are free to disclose mistakes or any issues they might have seen."

Training is a required part of compliance and its content and delivery are both important, says Alleyne. "It's good to have a practical dimension for training to be effective, like case studies, so that it isn't overly academic." He recommends organisations take steps to ensure that staff have properly understood their training by using tools like computerised tests and that they maintain training logs.

While the *FCA Handbook* includes a guide on financial crime, many organisations seek external support to help them handle the compliance burden. Some professional firms and compliance consultancies can advise on effective AML regulation compliance and help with investigations and prosecutions. They may also offer support like compliance technology and regulatory updates. Heather O'Gorman is head of payment services and financial crime at compliance specialist Thistle Initiatives. "Many of our clients are startups and can struggle to find the right level of operational staff. We help them establish their AML frameworks and controls," she says. This can include assisting with due diligence procedures and training programmes, she notes.

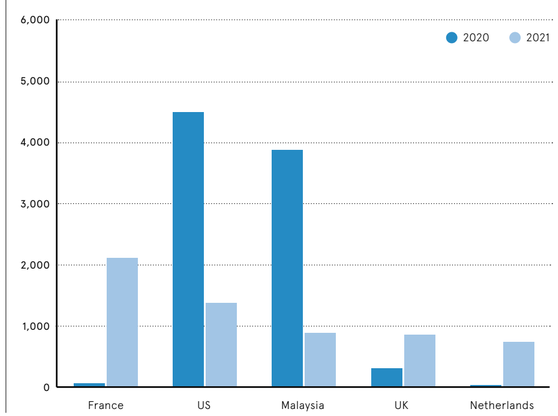
Tembo used FSCompliance to help it draft policies that complied with FCA guidance on AML regulations and to advise on how to establish and implement its compliance systems. "They've helped us compare our setup with those of their other clients, so that we can be best in class," say Dana and Riordan. It now uses FSCompliance on a retainer basis, which provides the organisation with a check-the-checker service. "It has been invaluable to have an adviser who has a detailed understanding of the application process and the ongoing regulatory system," they report.

For their organisation and others, such alertness and energy are what is required to meet the ongoing compliance challenge.

ANTI-MONEY LAUNDERING FINES HIT RECORD HIGHS

AML, sanctions, MiFID and data privacy fines by country ($m)

Fenergo, 2022

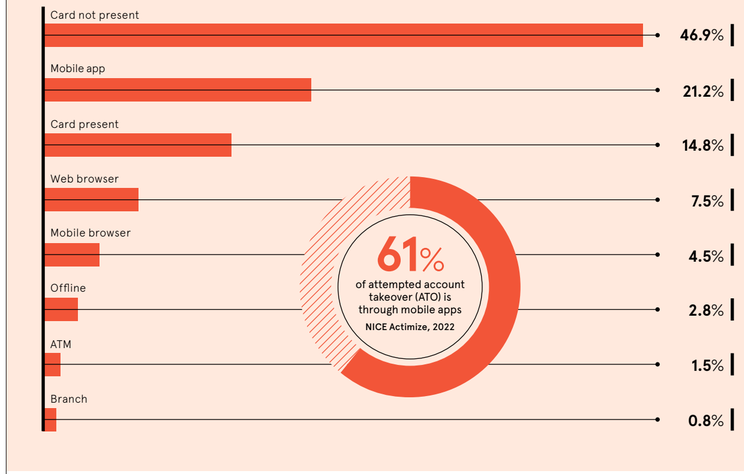


Preventing authorised fraud: the delicate balancing act of managing risk and customer experience

The UK is facing an epidemic of fraud. Financial institutions understand the gravity of the situation and are adapting to protect their customers while maintaining competitiveness in the market

ATTEMPTED FRAUD SHARE (%) ACROSS CHANNELS

NICE Actimize, 2022



A surge in social engineering scams, where victims are tricked into sending funds to fraudsters' accounts, is escalating. Banks and other payment providers face the perfect storm caused by the speed in which funds can be transferred and consumer demands for fast, frictionless payments. This has proven to be a fertile ground for criminals.

Such is the extent of these authorised push payment (APP) scams in the UK that they led to £583m in losses in 2021, according to UK Finance, a 40% increase compared with 2020. The trade association states that the country faces an "epidemic of fraud" and more action needs to be taken as cybercriminals quickly adapt their methods to suit shifting consumer lifestyles and behaviour.

Nearly 196,000 cases of APP fraud were reported in the UK last year in what UK Finance is calling a "national security threat."

"There's a very short time window – a matter of seconds – in which a bank or payment provider has to decide whether a transaction is genuine and either accept or decline. The reason why APP fraud is so hard to identify is because the victim initiates the transaction. The level of sophistication being employed for social engineering scams is now astounding, and the volume of attempts is on an unprecedented scale," explains Freddy Arthur, fraud strategy leader, EMEA, at NICE Actimize, a global market leader in financial crime and compliance solutions.

Through its Financial Services and Markets Bill, the UK government is working on legislation that makes banks and other payment providers responsible for reimbursing APP scam losses. Its aim is to ensure customers who are victims of fraud through no fault of their own are not left paying for it. Consequently, businesses will have to do more to protect their customers from this new wave of fraud.

"There's a lot of pressure on banks to get on top of this issue. Yet our relationship with our devices, banks and businesses from which we buy has evolved significantly, catalysed by the pandemic," says Arthur. "We've all automated and subcontracted whom and what we trust, with a key focus on technology. At the same time, we increasingly believe what we see on social media and the internet."

Arthur sees a widening gap between the growing amount of fraud and the ability to combat it. He says: "This creates an incredible opportunity for cybercriminals who aren't just engaging the younger generation, the digital natives, and Gen Z. Everyone is encountering these criminals. Regardless of digital fluency, British consumers are falling victims to these sophisticated scams at an alarming rate. This is not just an epidemic of fraud—it is an assault and an attack on our societal norms."

> **This is not just an epidemic of fraud—it is an assault and an attack on our societal norms**

At the same time, financial institutions are in a race to create the optimal customer experience, one that provides instant gratification to the purchaser and frictionless payments for businesses that want to facilitate sales, potentially disregarding possible risk in the face of competitive differentiation. It is not enough to be frictionless, businesses must provide a 'friction right' experience. It is an extremely fine balance between risk, trust and seamless authentication where expectations from all players have risen, along with the shift in liability to ensure the customer is being protected.

"We've seen banking operations teams double or even triple in number over the past three years to deal with the spiralling fraud associated with the exponential growth in digital transactions. The number of fraud alerts has spiked. It takes a lot of time to validate scams where victims have been socially engineered to make the payments themselves," explains Arthur.

"We've also seen a proliferation in point solutions by financial service providers to continually address new and emerging threats. It's critical to have a holistic view of risk or intelligent fraud prevention. This is why we use machine learning and AI to analyse billions of data points globally to scan transaction behaviours and spot anomalies."

Hundreds of key indicators – data gathered along every customer journey across a vast portfolio – can now be measured. These key indicators, embedded within advanced machine learning, can detect the known and unknown risks and evaluate anomalous behaviour for real-time decision-making.

"We have some of the largest pools of data worldwide and collective intelligence gathered from the largest global financial institutions. The combination of these sources enables our solutions to adapt to new and emerging threats," says Arthur. "To get ahead of this fraud epidemic, it's important to use a solution from a trusted provider. NICE Actimize is trusted because of our global expertise and ongoing innovation."

Go to niceactimize.com/emea to learn more about how the smartest AI can solve the most complex fraud

NICE · ACTIMIZE

Top financial institution reduces fraud loss by £4.6m

A top European financial institution with retail and commercial banking in the UK experienced a significant increase in fraud from social engineering scams brought on by an increase in digital activity and criminal sophistication. Fraudsters were also exploiting instant payments, such as peer-to-peer, because they provide quick cash transfers. In fact, scam tactics evolved so quickly that it strained the bank's ability to fight back.

NICE Actimize provided a layered approach to fraud prevention that gave the business a comprehensive view of customer risk. By leveraging a powerful combination of data intelligence, machine learning and AI, the firm was able to identify customers who might be more vulnerable to scams. Specific social engineering scams were also identified, while purpose built machine learning models were able to cover a broad spectrum of fraud typologies.

The value detection rate went up by 200% versus legacy models, while fraud loss for scams was reduced by £4.6m in one year.

Commercial feature

Tackling financial crime through collaboration

Taking a joined-up, data-led approach is key to addressing the rising problem of financial crime

Financial crime is a multi-trillion-dollar business for criminal organisations. Annually, the proceeds from their illicit activity laundered through global financial networks are worth between 2-5% of global GDP. As a result of the loss and harm this is causing society, fighting financial crime has become a key priority for many governments, including in the UK.

Just to remain compliant, financial institutions have been investing heavily in their financial crime programmes for the last 20 years. At the same time, the costs of compliance have continued to rise exponentially. Despite all this investment, driven largely by regulatory pressure, it's not enough. The value of illicit funds confiscated or disrupted is still well below acceptable levels and more needs to be done to tackle the problem.

The challenge for firms is to both create a more effective financial crime programme and drive efficiency. What may look like two competing agendas can, however, be delivered using technology and data. With a big focus by regulators and policymakers on technical compliance as well as demonstrating effectiveness in disrupting financial crime, alongside an internal agenda on cost optimisation, the spotlight on digital transformation has never been stronger, says Geraldine Lawlor, global head of financial crime for KPMG.

More mature organisations are currently moving towards data and technology-enabled process transformation. This is where the future appears to be. However, it requires some brave decisions to be made on legacy infrastructure. It also requires a move away from the silo mentality, bringing the organisation together in terms of how it views and manages this risk. For some, this may be a paradigm shift, but for others, it's a necessity.

To support this change, the traditional limitations on data from product-led legacy systems are being overcome by tools that leverage and enrich existing data sets. This allows the data to be used more effectively. "Banks are also moving from traditional approaches to monitoring transactions to looking at networks of activity, connecting relationships and observing illicit activity across a network that was not evident at a transactional level," says Ignatius Adjei, UK fraud technology lead at KPMG.

The focus on data is fast becoming a fundamental part of how organisations better manage their financial crime risks. Their know your customer (KYC) programme is at the heart of this. "Rather than see it as an exercise in identification and verification aligned to technical minimums, it should be viewed as the data source to manage all subsequent downstream processes that support better detection, disruption and optimisation," says Lawlor.

Another emerging theme is convergence under an economic crime lens. This covers a collection of risks; namely fraud, money laundering, counter-terrorism, market abuse, sanctions, bribery and corruption and tax evasion. It is a means by which organisations are starting to recognise that managing risks in isolation is not the answer. They need to have a new way of assessing how to deliver greater efficiency.

"We are seeing this convergence, with fraud and cyber-enabled crime moving closer to anti-money laundering, particularly around mules," says Adjei. This is reflected in the mindset shift towards the need for greater collaboration. It's supported by access to enriched data, information and intelligence, and enabled by better tools. As a result, firms' ability to manage risks and threats is improving.

With the focus on innovation and cost optimisation, the role of the compliance function is also evolving. There is an increasing trend towards moving activity out of compliance and into shared services. Doing so enables firms to drive operational standardisation and convergence, leveraging common tools and management structures, and positioning for greater efficiency.

However, this transition can have its challenges, and "it is important to set clear outcomes, good design principles and agreement around how accountability, responsibility and oversight need to work," says Lawlor. "It is, however, worth the effort, as it brings an organisation together and makes the business accountable for client risk. It also allows compliance to move to an oversight role, while driving an optimisation agenda through operations, leveraging data and technology to full effect."

Alongside the work currently being undertaken within organisations, regulators are also playing a key role in supporting and encouraging innovation to better manage the negative effects of financial crime. As organisations start to improve the way they respond to and work with their regulators, these relationships will evolve positively. "When you start to bring them into the conversation, there becomes a real opportunity to drive a much healthier relationship where we are all on the same side. We're part of an eco-system that is working together against the common threat: the criminal," says Lawlor.

To further support collaboration, there has been an emergence of public-private partnerships across a number of jurisdictions, with the UK taking the lead. Reform is also high on the agenda, underpinned by the legal changes coming through under a series of economic crime bills. A key component of such reform will be the ability to share information and intelligence more routinely and to put it to use. There's already a huge amount of work underway here. Without it, the ability to join the dots across the financial marketplace and, ultimately, disrupt criminal networks remains limited.

Success in driving down the negative effects of financial crime comes from the will of all the stakeholders to change and evolve collectively. It's amazing what can be achieved when everyone pulls in the same direction. The loss and harm to society needs to stop, and our economies need to be able to prosper and grow. Moving forward to an environment built on collaboration, enabled by data, intelligence and the right tools, will be critical to achieving this.

2–5%

of global GDP comes from the proceeds of criminal organisations' illicit activity laundered through global financial networks each year

> **The loss and harm to society needs to stop, and our economies must be allowed to prosper and grow**

For more information about financial crime visit home.kpmg/uk/en/fincrime

KPMG

REGULATION

Crypto-crime crackdown increases

Enforcement actions are increasing as global regulators step up their efforts to supervise the crypto market, while some jurisdictions are adopting a more crypto-friendly approach

Ben Edwards

Yuichiro Chino via Getty Images

With the value of the global cryptocurrency market north of $3tn (£1.09tn) and mainstream crypto adoption continuing to accelerate, global regulators are racing to keep up.

In March, President Joe Biden signed an executive order that tasks the entire US government with forming a strategy to regulate digital assets, including cryptocurrencies. Meanwhile, in Europe the EU is in the process of finalising its markets in crypto assets legislation, which seeks to oversee crypto activities that fall outside existing regulations. The UK's FCA also earlier this year proposed tougher rules on crypto advertising, to stamp out false or misleading claims.

"Those who are new to this or just pressed for time will say crypto is unregulated – nothing could be further from the truth," says Marco Santori, chief legal officer at Kraken, a crypto exchange.

Much of the early regulatory agenda for cryptocurrencies and the emergence of blockchain technology focused on money services, though since 2017 with the boom in initial coin offerings, that has started broadening into areas such as capital formation, says Santori.

"There are new, emerging uses of blockchain technology that implicate new risks and are creating new industries – it's those emerging uses that are under regulatory scrutiny," he says.

But given the rapid pace of crypto adoption, regulators have struggled to keep pace. "Regulation has lagged but as Biden's order indicates, there is a growing awareness that there needs to be a much tighter regulatory framework around crypto," says Ben Richmond, founder and CEO of regtech company Cube Global.

Enforcement actions are also starting to increase. The US Securities and Exchange Commission (SEC), for instance, has brought around 100 cryptocurrency enforcement actions since 2013. The agency's new chairman, Gary Gensler, said the SEC hopes to start regulating crypto exchanges this year.

> **New uses of blockchain technology implicate new risks and are creating industries. It's those emerging uses that are under regulatory scrutiny**

> "Learnings from those actions are driving regulator behaviour, but that's where it risks becoming fragmented because you can end up with different approaches to the same problem," says Richmond.

Another debate has fizzed around how to regulate crypto. Should it be bolted on to existing regulations or regulated as a separate industry, with its own regulator and laws? Timothy Spangler, a US-based partner at law firm Dechert, believes it should be the former.

"I would rather spend more time understanding the technological impacts than creating new regulators, new crimes and new oversight mechanisms, and then having to debug those over the course of years and years," he says. "That could unnecessarily stymie innovation."

Others argue that the novelty of blockchain technology means it shouldn't be shoe-horned into current regulations.

"Most regulators are using a traditional approach to regulate crypto," says William Je, CEO of Hamilton Investment Management. "But crypto is creating new financial products that are entirely different to anything that has come before."

Some jurisdictions are taking a more active pro-crypto stance to attract crypto businesses, such as US state Wyoming, which has passed a series of crypto-friendly blockchain laws.

"Wyoming has taken a descriptive rather than a prescriptive approach to regulation and is a model for other jurisdictions," says Santori.

One initiative Wyoming has adopted is creating a banking license that tailors the regulatory regime to the actual risks of the bank. For instance, Kraken was the first crypto company to receive a license under the state's new banking charter aimed at digital asset businesses, which allows them to take deposits as opposed to make loans. "It dials up oversight of reserves and forgoes the regulations usually required for banks that lend," says Santori.

A focus on crypto-mining activities, particularly around energy use, is also attracting the attention of regulators. China has banned crypto mining, while the EU considered banning certain energy-intensive methods for mining crypto but has since backed down.

"To say that we need to regulate crypto miners is to say that crypto mining poses a danger, but we're a long way from quantifying that," says Spangler. "How comfortable are we that we accurately know the energy usage that miners engage in? Most of the academic surveys are qualified and speculative."

While regulatory best practice is a work in progress, Spangler believes those jurisdictions that tread cautiously are likely to yield more effective long-term outcomes.

"We need to move at the right pace to make good decisions," he says. "We want to move forward based on knowledge. Move slowly and roll out things as needed – we don't know where blockchain will move."

But while the US has traditionally set the standard for global financial regulation, it is not a given that it will shape how crypto regulation develops worldwide.

"Most people would agree that crypto's centre of gravity initially was the US and Canada. But there's no reason why, having created a new technology or protocol, they would also win the deployment," Spangler comments.

A lack of regulatory harmonisation across jurisdictions is also potentially weighing on the growth of the crypto market."Every country has different rules and regulations – or even definitions – of what should be regulated, so at the moment it's not clear, which is holding back institutional investors from investing in crypto," says Je. "This is the biggest hurdle for the development of crypto, so we need more clarity."

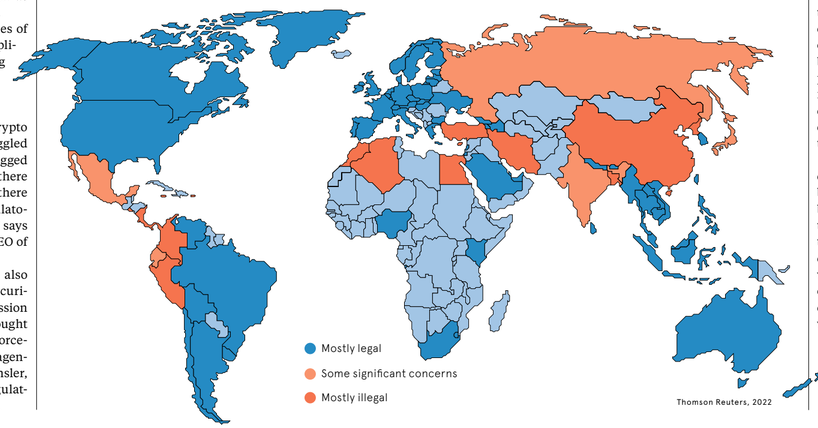
Others believe that while regulation is necessary to safeguard consumers, it could slow the pace of adoption. "It's about getting the balance right. How do you protect people but enable this world to flourish?" says Richmond. "The concern is that if the regulation comes in too hard, it will slow down the uptake."

Worries that too much regulation could choke innovation are likely to be overblown, though Santori believes some innovation will inevitably be constrained as regulators tighten their grip. "That's the trade-off when we regulate," he says. "But we also create a more stable and welcoming environment, so that is the correct lens to view the decision of whether to regulate."

As blockchain technology continues to thrive and new use cases emerge, one thing is certain: the regulatory backdrop is far from resolved.

CRYPTO REGULATION WORLDWIDE

Level of cryptocurrency regulation by country



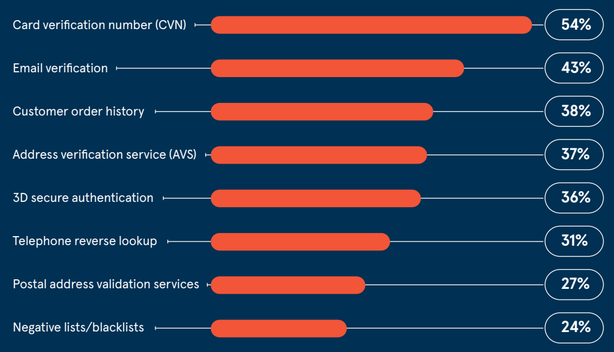
Thomson Reuters, 2022

THE RISE OF ECOMMERCE FRAUD

European etailers lost a reported 3.2% of their revenue to payment fraud in 2021 as Covid made ecommerce a fertile new battleground for scammers. So how big a problem is online retail fraud, what are companies doing to protect against it and just how badly are customers being affected?

TOP TOOLS ECOMMERCE COMPANIES CAN USE TO STAY SAFE

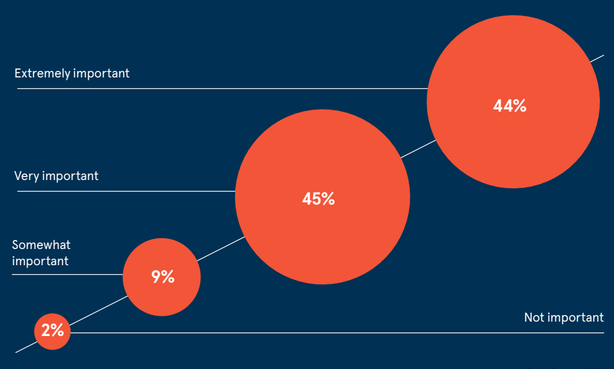
Most common fraud detection tools used by online merchants worldwide in 2021



CyberSource, 2021

ARE ONLINE RETAILERS TAKING FRAUD SERIOUSLY ENOUGH?

Importance of ecommerce fraud management to overall strategy to companies worldwide

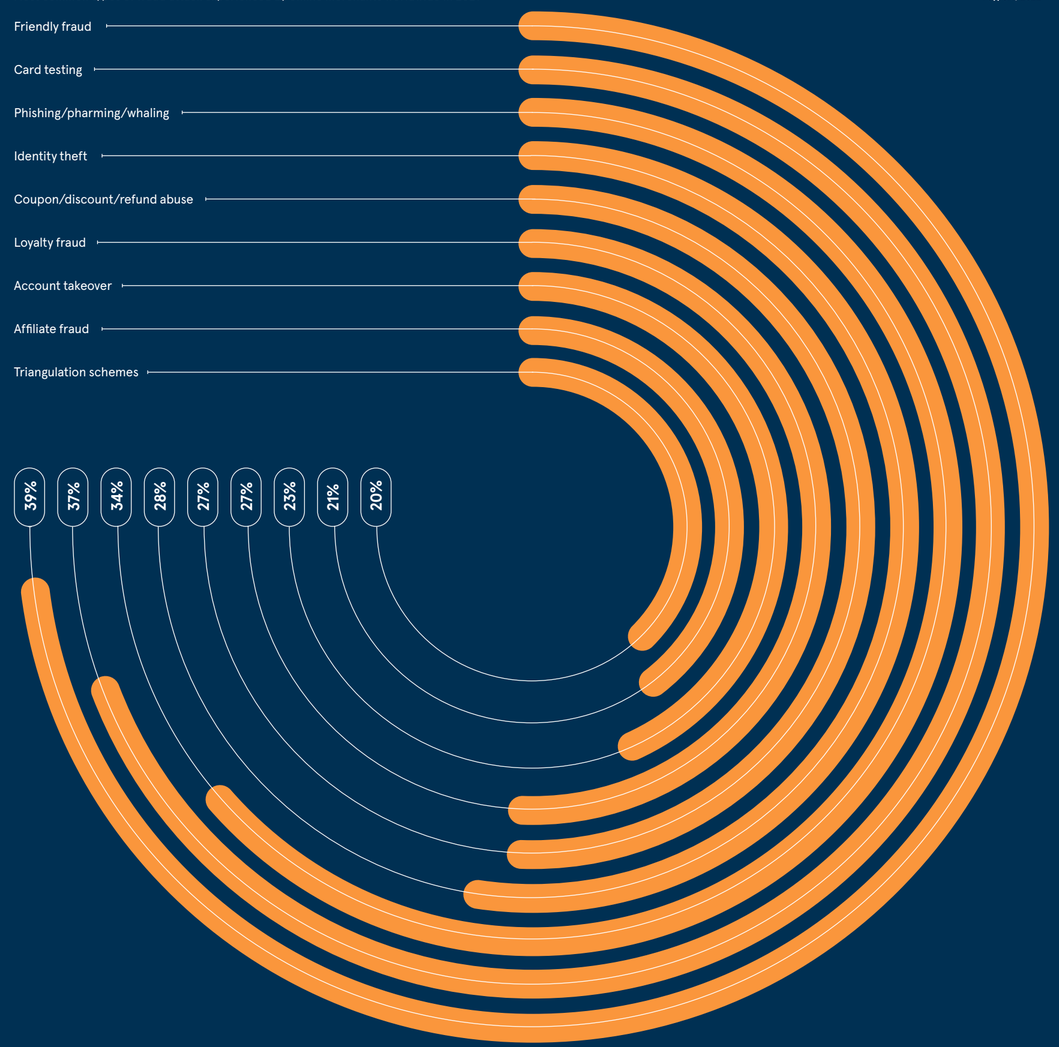


CyberSource, 2021

WHAT SHOULD RETAILERS BE WATCHING OUT FOR?

Most common types of fraud attack experienced by online merchants worldwide in 2021

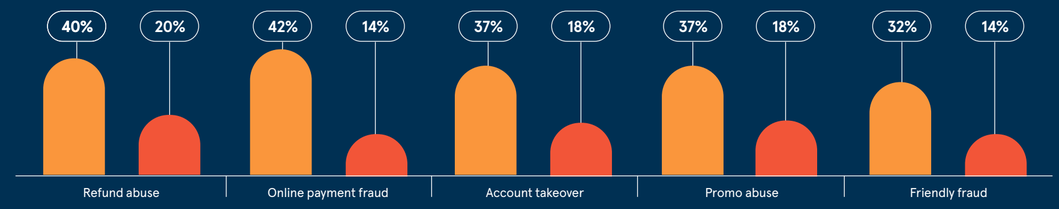
Paypers, 2022



ECOMMERCE FRAUD IS ON THE RISE

Change in fraud levels experienced by online merchants worldwide in 2021 ● Increase ● Significant increase

Qualtrics and Ravelin, 2022



$17.5bn

lost to online payment fraud worldwide in 2020

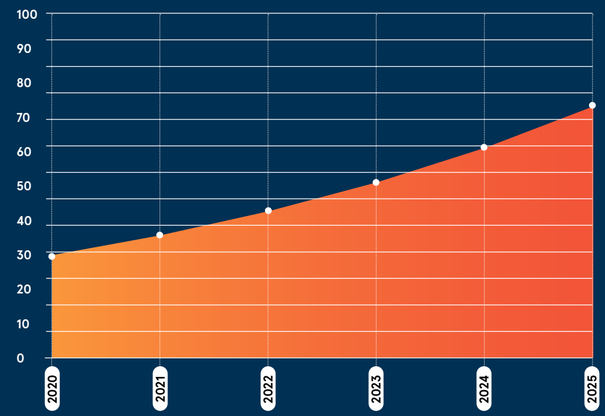
$20bn

in 2021

Juniper Research, 2021

WILL DEMAND FOR SOLUTIONS CONTINUE TO GROW?

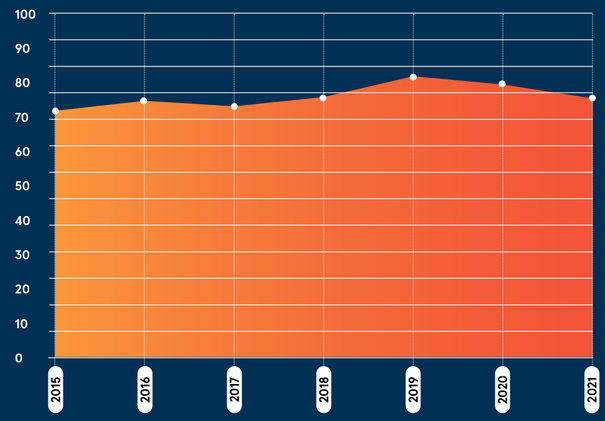
Ecommerce fraud detection and prevention market size worldwide from 2020 to 2025 ($bn)



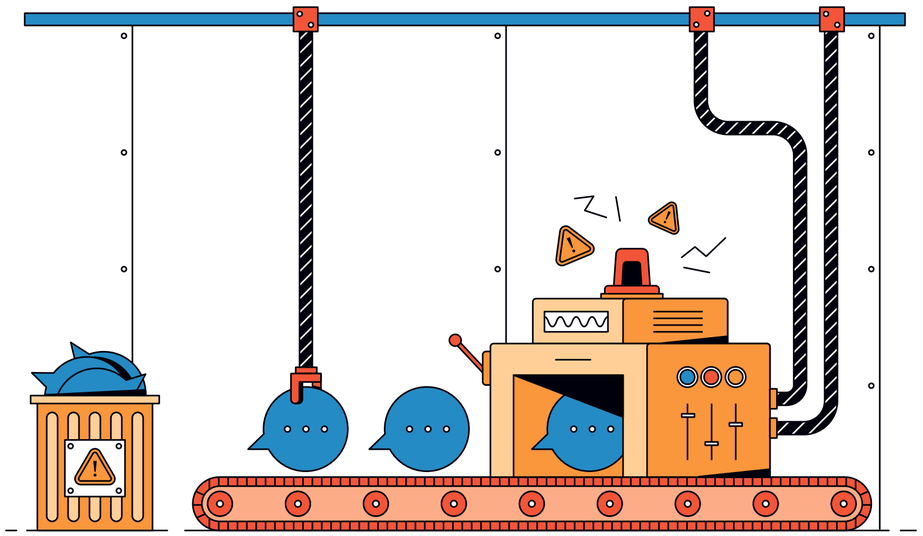
ReportLinker and Statista, 2021

HOW ECOMMERCE FRAUD HITS CUSTOMERS

Percentage of online shopping scam victims who lost money from these attacks worldwide



BBB, 2021



ARTIFICIAL INTELLIGENCE

Conversational AI has joined the chat

Organisations are using new technology to analyse the voices of those posing as customers in real time while reducing false positives

Oliver Pickup

Great Britain is the fraud capital of the world, according to a *Daily Mail* investigation published in June. The study calculated that 40 million adults have been targeted by scammers this year. In April, a reported £700m was lost to fraud, compared to an average of £200m per month in 2021. As well as using convincing ruses, scammers are increasingly sophisticated cybercriminals.

If the UK does go into recession, as predicted, then the level of attacks is likely to increase even further. Jon Holden is head of security at digital-first bank Atom. "Any economic and supply-chain pressure has always had an impact and motivated more fraud," he says. He suggests that the "classic fraud triangle" of pressure, opportunity and rationalisation comes into play.

Financial service operators are investing in nascent fraud-prevention technologies such as conversational AI and other biometric solutions to reduce fraud. "Conversational AI is being used across the industry to recognise patterns in conversations with agents or via chatbots that may indicate social engineering-type conversations, to shut them down in real time," continues Holden. "Any later than real time and the impact of such AI can be deadened as the action comes too late. Linking this to segmentation models that identify the most vulnerable customers can then help get action to those who need it fastest and help with target prevention activity too."

This last point is crucial because educating customers about swindlers is not straightforward. "Unfortunately, there will always be vulnerable people being scammed," Holden says. "The banks are doing a lot of work to identify and protect vulnerable customers, but clever social engineering, often over a long period, will always create more victims of romance scams, investment scams, or purchase scams when victims send money for goods never received."

AI is a critical tool to fight fraud. Not only does it reduce the possibility of human error but it raises the flag quickly, which enables faster, smarter interventions. Additionally, it provides "far better insight of the cyber ecosystem", adds Holden, "almost at the point of predictive detection, which helps with both threat decisioning and threat hunting".

> **Since our initial implementation of AI three years ago, the improvements to alert quality have been incredible**

Jason Costain is head of fraud prevention at NatWest, which serves 19 million customers across its banking and financial services brands. He agrees it is vital for conversational AI to join the chat. Because the call centre is an important customer service channel and a prime target for fraudulent activity – both from lone-wolf attackers and organised crime networks – he resolved to establish more effective security mechanisms, while delivering a fast, smooth experience for genuine customers.

In late 2020, NatWest opted for a speech recognition solution by Nuance, a company which Microsoft recently acquired. It screens every incoming call and compares voice characteristics, including pitch, cadence, and accent, to a digital library of voices associated with fraud against the bank. The software immediately flags suspicious calls and alerts the call centre agent about potential fraud attempts.

Before the end of the first year of deploying the Nuance Gatekeeper system, NatWest had screened 17 million incoming calls. Of those, 23,000 led to alerts and the bank found that around one in every 3,500 calls is a fraud attempt. As well as a library of 'bad' voices, NatWest agents now have a safe list of genuine customer voices that can be used for rapid authentication without customers needing to recall passwords and other identifying information. That knowledge enables the bank to identify and disrupt organised crime activities, to protect its customers and assist law enforcement.

"We're using voice-biometric technology to build a clear picture of our customers' voices and what criminal voices sound like," Costain says. "We can detect when we get a fraudulent voice coming in across our network as soon as it happens. Using a combination of biometric and behavioural data, we now have far greater confidence that we are speaking to our genuine customers and keeping them safe."

He estimates the return on investment from the tool is more than 300%. "As payback from technology deployment, it's been impressive. But it's not just about stopping financial loss; it's also about disrupting criminals." For instance, NatWest identified a prolific fraudster connected to suspect logins on 1,500 bank accounts, and an arrest followed.

"For trusted organisations like banks, where data security is everything, the identification of the future is all about layers of security: your biometrics, the devices you use, and understanding your normal pattern of behaviour," adds Costain. "At NatWest, we are already there, and our customers are protected by it."

There are other benefits to be gained by investing in conversational AI solutions. Dr Hassaan Khan is head of the School of Digital Finance at Arden University. He points to a recent survey that indicates almost 90% of the banking sector's interactions will be automated by 2023. "To stay competitive, organisations must rethink their strategies for improved customer experience. Banks are cognisant that conversational AI can help them be prepared and meet their customers' rising demands and expectations," he says.

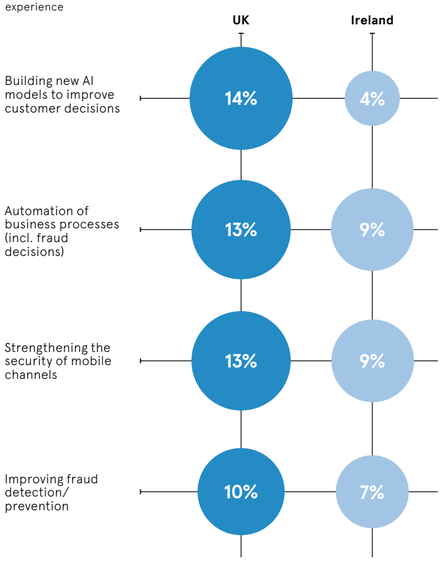
This observation chimes with Livia Benisty. She is the global head of anti-money laundering at Banking Circle, the B2B bank relied on by Stripe, Paysafe, Shopify and other big businesses, responsible for settling approximately 6% of the world's ecommerce payments. "With AML fines rocketing – in 2021, the Financial Conduct Authority dished out a record $672m (£559m) – it's clear that transaction monitoring cannot cope in its current state," Benisty says. "That's why adopting AI and machine learning is vital for overturning criminal activity."

She argues, however, that many in the financial services industry are reluctant to invest in the newest AML solutions for fear of being reprimanded by regulators. "If you're a bank, you come under a lot of scrutiny and there's been resistance to using AI like ours," she says. "AI is seen as unproven and risky to use but the opposite is true. Since our initial implementation of AI three years ago, the improvements to alert quality have been incredible. AI alleviates admin-heavy processes, enhancing detection by increasing rules precision and highlighting red flags the naked human eye could never spot."

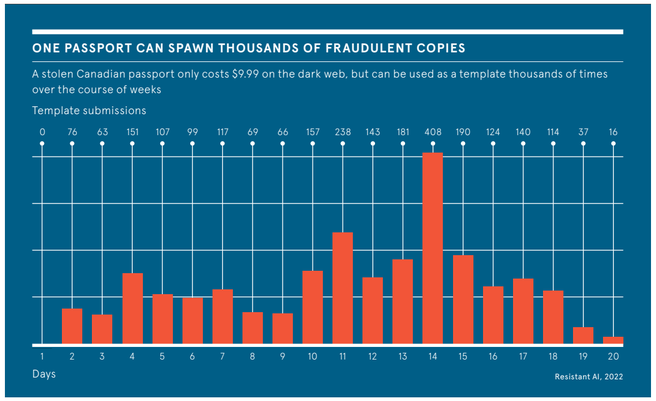
> **Unfortunately, there will always be vulnerable people being scammed**

Even regulators would be impressed by the results revealed by Banking Circle's head of AML. More than 600 bank accounts have been closed or escalated to the compliance department, thanks to AI-related findings. Further, the solution "dramatically reduces" the so-called false positive alerts. "It's well known the industry can see rates of a staggering 99%," adds Benisty. "In highlighting fewer non-risky payments, fewer false positives are generated, ultimately meaning more time to investigate suspicious payments."

As the economy weakens, and criminals grow stronger, financial services operators would be wise to dial up their conversational AI capabilities to improve customer experience today and pave the way to a password-less tomorrow.



Commercial feature



Financial fraudsters face crackdown

Criminal gangs are creating fraudulent accounts in financial services at an incredible scale. But machine-learning technology is foiling these attempts and exposing the bad actors behind them

Financial cyber fraud is getting out of hand. As a new generation of banks and financial brands launch digital services, fierce competition to sign up new customers is making it easier than ever to open accounts. It can be as simple as uploading photos of your passport, proof of address, and a selfie holding up a handwritten sign with a predetermined code to affirm you are "not a robot."

And that ease provides explosive opportunities for criminals to create fraudulent sign-ups at an alarming rate. By some estimates, one in four new accounts is fraudulent.

Single identities are still being stolen to conduct fraudulent transactions such as taking out loans, falsely claiming insurance, or for money laundering. But it's now more cost-effective to use those identities as templates for a whole series of forged identities that can overwhelm onboarding controls.

Scale of serial identity fraud over a 3 month period, a single institution found:

964
document templates used in serial fraud attacks

11,214
fake identities created from those templates

Resistant AI, 2022

"We've seen a dramatic increase in fake robotic identities being onboarded in financial services. And given that it is automated, it is very easy to scale up," says Martin Rehak, chief executive of Resistant AI. "Criminals have largely abandoned traditional face-to-face fraud in favour of serial, automated fraud," he adds.

He says the gangs are using "fraud as a service," which packages and sells many of the same automation tools and services used by fintechs to criminals looking to engage in fraudulent activity.

But Rehak says Resistant AI is making life hard for these gangs. Its system looks across all the identification documents and behaviours in a financial service's onboarding process and then applies what Rehak calls "identity forensics" to find fraudulent sign-ups.

For instance, Resistant AI's machine-learning system may detect the same crease, in the same place, across a series of ID photographs, indicating that each document was edited from a single source image, an obvious case of serial fraud. Looking at similarities in the lighting and background of photographs of documents can also indicate if different identities are all being uploaded by the same fraudster. Resistant AI also analyses behavioural biometrics of things like the keystrokes made when filling in an application form. Too high a speed might indicate automation could be at work.

Rehak says the company's algorithms check hundreds of elements of onboarding documents and behaviours to uncover cases of serial fraud.

"While many companies promise to stop attacks, what we do is hunt down the source – the enabling assets," he says. "When a criminal makes a mistake with one identity – perhaps a fraudster wants less strain on their eyes so uses a green light that colours the documents – we look for it across all others and unravel the whole operation."

"We impose friction back onto the criminals and make them work so hard on operational security to avoid all those mistakes they have to become bureaucratic compliance officers. It ramps up their costs and makes it impossible to scale their attacks."

In one financial services company alone, Resistant AI found over 900 document templates being used for thousands of fake identities over the course of a quarter. This is why Rehak believes identity fraud at account opening could eventually reach the volume of spam, which accounts for up to 85% of emails. "Fintechs must use the latest technology to track down serial, automated fraud and make these gangs miserable. This requires pairing human insight with automated detection" he says.

The challenge for financial services are departmental and competitive silos. Cybercriminals prey on this lack of data sharing, so allowing solutions to look across organisations to locate fraudulent behaviours is vital.

The future of the finance industry will depend on using software to weed out malicious activity and keeping fraudulent sign-ups to a minimum. This is an era where machines battle other machines to root out criminal activity.

For more information please visit resistant.ai

RESISTANT.AI

CYBER RESILIENCE

Five cyber scams to avoid now

Cyber attacks are on the rise. Knowing how to spot the warning signs makes it easier to avoid becoming a victim

Chris Stokel-Walker

To succeed in business, it has been said, you need sharp elbows and a hard head. But as well as the need to fend off competitors, vigilance for cyber attacks – and knowing how to sidestep them – is now high on the agenda of all business leaders.

Cybercriminals might be quick to devise new and increasingly sophisticated scams, hacks and fraud schemes but there are recognisable patterns. Experts reveal the top five most common types of cyber attacks to look out for.

1 Phishing

Phishing is an email or a text message spoofing an organisation or person. The aim is to trick the would-be victim into clicking on a link and entering their bank details. HMRC is commonly used in phishing attempts for organisations, while for individuals, holiday companies are the bait.

"All organisations need to deal with the threat of phishing because it's used in most cyber attacks," says Jessica Barker, co-founder and co-CEO of Cygenta, a cybersecurity consultancy. "Since technical defences have improved, cybercriminals have realised that attacks on organisations are easier, faster, cheaper, less risky and more likely to succeed when they include phishing."

Action Fraud highlights and tracks cybercrime in England, Wales and Northern Ireland. It recently highlighted an increase in phishing attacks on individuals by criminals pretending to be holiday companies with too good to be true offers. "Whenever demand for holidays soars, so does the number of scams," observes Pauline Smith, head of Action Fraud.

2 Business email compromise (BEC)

Phishing is a fundamental but small part of a set of fraud-launching platforms that target businesses. "The biggest business crime is BEC, business email compromise," says Alan Woodward, professor of cybersecurity at the University of Surrey. "It's the move from simple phishing through spear phishing to whaling, which draws in C-suite levels."

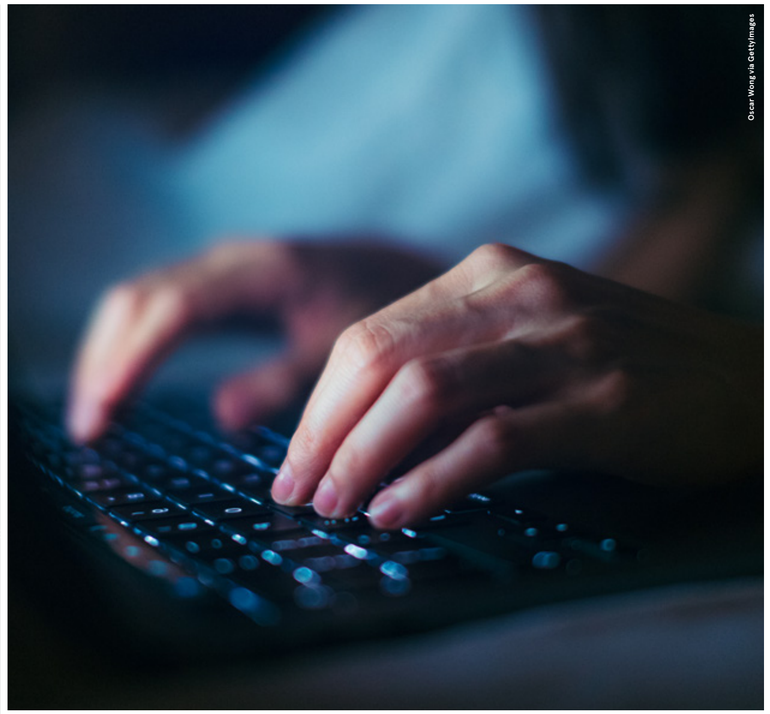
Spear phishing is a targeted version of phishing: hackers select a company or individual to attack. Whaling is a step further than spear phishing. The target here is the individual believed to hold the keys to the kingdom of the company's secrets.

A successful BEC tends to stem from social engineering or convincing someone that a hacker is whom they claim to be. Businesses need to give digital literacy training to staff at all levels. For Woodward, that means understanding the likelihood of being targeted and the ability to recognise suspicious emails. That could include checking whether the URLs in emails or text messages match the official websites. Or, if the payroll department emails a request for the company's bank account password, confirming the request offline by picking up the phone and speaking to the alleged sender. It could make all the difference between avoiding the worst or falling foul of a hack.

3 Ransomware

"Ransomware is the crime most organisations need to prepare for and is the most difficult to recover from," warns Woodward. "Businesses have to assume it's a case of when – not if – it'll happen and have a business continuity plan that allows the business to continue to operate and to reinstate a trusted version of the systems and network."

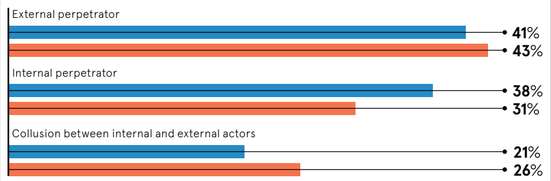
Ransomware isn't new, but it is increasingly sophisticated as cybercriminals change their methods to infiltrate networks and databases. "Ransomware has evolved," says Barker. "In many cases, cybercriminals don't just encrypt their victims' data. They also threaten to publicly leak it if the ransom isn't paid."



Oscar Wong via Gettyimages

WHERE THE THREATS ARE COMING FROM

Main perpetrator of the most disruptive or serious fraud experienced — 2020 — 2021



PwC, 2022

The potential lucre that criminals can gain from ransomware is so great that it has spawned its own mini-economy. Ransomware as a service is a niche but growing area in which criminals sell ransomware 'packages' on the dark web. This allows other criminals to launch ransomware attacks without needing any technical skill. It also means businesses can be bombarded with ransomware attempts, sent through email attachments and getting people to click on compromised websites that secretly download a virus that locks all files.

Prevention is the best cure, with good training to ensure people don't fall victim to such ploys. But the scale of ransomware attacks makes them almost an inevitability. That poses its own problems. "Many businesses have relied on insurers paying up the ransom, but that has two issues," explains Woodward. "Criminals' decryption tools are often terrible, and it's quicker to rebuild – as the Irish Health Service discovered when it was attacked in May 2021. And insurers certainly won't pay out if you haven't taken reasonable measures to mitigate losses."

4 Remote access tools (RAT)

Nobody likes rats, especially in cybercrime. Remote access tools (RATs) were responsible for £57m in losses in 2021, according to Action Fraud. It's a simple scheme, but fraudulent at its core.

The scam often begins with someone calling a company, claiming to be a representative of a trusted supplier or business partner. They could also pretend to be calling from the victim's bank to investigate a suspicious transaction on the account. They'll be deliberately confusing about the trail of actions required before offering a simple solution: to do it for them if the victim gives them remote access to their computer.

Once in, the criminal siphons off vital data and often drains any bank accounts open on the victim's computer. It's a crime often used to target individuals but can offer even bigger payloads when it targets businesses. "Only install software or grant remote access to your computer if you're asked by someone you know and trust," warns detective chief inspector Craig Mullish from the City of London Police.

5 Insider threats

Some of the biggest risks are from hackers trying to access a company's IT systems. But not every attack is launched from outside a company. "Organisations must be aware that incidents and breaches often come from internal as well as external sources," cautions Barker.

And insider attacks are severely effective. "They know the information to target and if they're successful, it can shake confidence in the organisation and damage its reputation," she says. Keeping your workers happy is vital – and keeping track of them could prevent headaches down the line. ●

> Ransomware is the crime that most organisations need to prepare for and is the most difficult to recover from

INSIGHT

'The rise in the cost of living is giving criminals opportunities to scam those in need'

As cases of fraud continue to rise, chief executive of fraud prevention not-for-profit Cifas, **Mike Haley**, explores what is driving this

Q What are the Cifas databases?

A Cifas's fraud databases are the largest and most comprehensive sources of fraud risk data in the UK. Hundreds of thousands of records are added each year by Cifas members, and this data and intelligence are shared online in real time.

Our National Fraud Database holds records of fraud risk such as account takeover, identity fraud, false insurance claims, false applications and more, and organisations who use it prevent over £1bn in fraud losses every year.

Q What are some of the biggest fraud trends we are seeing this year and what is driving them?

A Instances of fraud continue to rise each year, and already we are seeing nearly 200,000 cases of high-risk fraudulent conduct recorded, up 11% on 2021.

The majority of cases relate to identity fraud, which is up a third from last year, with banking and plastic cards heavily targeted by criminals who use stolen details to apply for products and services.

Nearly a fifth of cases relate to money muling, where a person allows their account to be used, often to launder the proceeds of crime. Although most of these cases occur in the 21-30 age group, this year we're seeing a rise among 31-40 year-olds.

Recent research by Cifas showed that 17% of the public believed this type of activity was 'reasonable', so I'm concerned that people may be tempted to use this as a legitimate way to supplement their income during times of financial insecurity.

Fraud by staff against their employer is also on the rise, with cases filed to our Internal Fraud Database up by almost half from 2021. Most of these relate to individuals working in contact centres, and we know that criminals have been targeting these workers to gain access to accounts and obtain personal data.

Q To what extent is the cost-of-living crisis exacerbating already prevalent threats?

A It is providing criminals with new opportunities to scam those in need, from advanced fee fraud and obtaining loans, to investment scams attracting those looking for ways to supplement their income.

The economic crisis is also an opportunity for scammers to steal personal and financial information. Recently we've seen a rise in consumers being targeted by phishing campaigns, for example purporting to be from utility providers offering savings on energy bills or emails offering fuel vouchers, fake jobs and money-making opportunities. These emails are becoming increasingly sophisticated.

Criminals are also pretending to be from legitimate firms seeking to persuade victims to share their computer screen using remote access desktop services, and then stealing information to apply for products and services in their name or to take over their bank accounts.

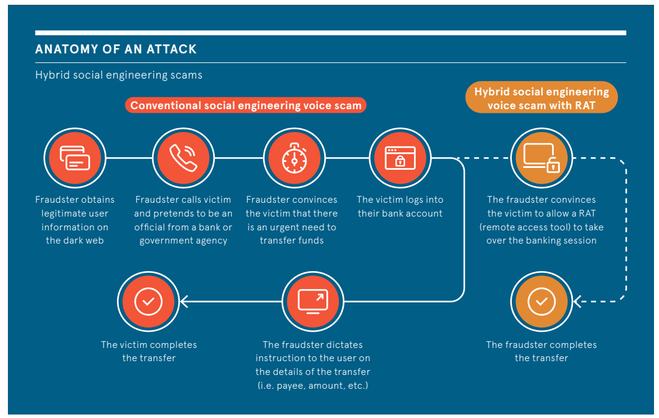
But it's not just consumers being targeted. Businesses too are increasingly finding themselves under greater attack from criminals.

With an increasing number of companies looking for ways to expand their portfolio into the buy-now-pay-later space, fraudsters will look for ways to exploit any vulnerabilities within their processes.

In addition, remote working is increasing the threat of criminals paying staff to make changes to accounts or sell data. We've also seen a rise in false employment applications, with individuals failing to disclose adverse credit or gaps in their employment history, believing it will hinder their hiring opportunity. Cifas research has revealed that one in eight people believe that lying on their CV is 'reasonable', which poses a serious risk to a business and its staff. More than ever, organisations must ensure they perform rigorous checks through the employee lifecycle to identify fraud risks. ●

Mike Haley
CEO, Cifas

Commercial feature



Outsmarting the scammers

Behavioural biometric technology can prevent fraudulent scams by detecting even the subtlest behavioural changes

Financial scams are evolving on a continual basis and becoming ever more sophisticated, making it even harder for banks and consumers to keep up.

What started as hacking accounts to steal passwords has evolved into what's commonly known as social engineering. Technically referred to as authorised push payment (APP) fraud, it involves the scammer using personal information to gain the victim's trust and psychologically manipulating them to then secure banking credentials or transfer funds to them.

In the first half of 2021, criminals stole a total of £753.9m through fraud in the UK, a 30% increase year on year, according to UK Finance, as cases of APP fraud saw a sharp increase. These scams have become so elaborate that criminals can easily circumvent one-time password authentications via SMS.

There are a host of different attack vectors too. These include phishing, where the target is asked to click on a link that then uses malware to steal the data. Vishing attacks involve an impersonator calling up and requesting updates or personal information, while smishing uses SMS to infect a device with malware, or encourage the individual to share information or unwittingly give it away by going through a multi-factor authentication.

Successful social engineering attacks require a victim taking action upon request from the criminal direction. Two examples of this are malicious payee scams and malicious redirection. The first involves duping the victim to buy items that either don't exist or are never received, while malicious redirection uses a fake or forged persona to trick the victim into transferring funds into a money mule account or an account the cybercriminal controls.

As soon as the money is received it is dispersed to multiple accounts, usually abroad, and then either cashed out or transferred to cryptocurrency, making it difficult for banks to trace and recover. The advent of instant payments has only compounded the issue.

"Cybercriminals feed on people's fear and anxiety to prize sensitive information away," says Gadi Mazor, CEO of BioCatch. "The Covid-19 pandemic and cost of living crisis have acted as a hotbed for cybercrime and specifically social engineering attacks."

Stolen personal information can be used to open a fraudulent bank account, take over an existing one or to manipulate the user into transferring their own funds to the cybercriminal. The consequences of becoming a victim of these scams can be devastating, not only financially but reputationally too.

As the criminals become smarter in their techniques, businesses must stay one step ahead. While companies have introduced additional layers of security, such as longer passwords and two-factor authentication, to protect against scams, these often detract from user experience and don't provide protection against sophisticated social-engineering scams.

> Scammers capitalised on the pandemic, which gave rise to a multitude of unusual financial transactions

To overcome the new breed of fraud without impacting experience, BioCatch has established an AI-based solution that analyses behavioural insights and patterns to uncover scams. By using AI and machine learning, it analyses a range of different factors, such as how users are holding their device or the speed a password is typed in, to detect suspicious activity. During an average session it analyses more than 2,000 distinct data points.

The technology then compares the user's activity with the known individual's typical behaviours to see if they are consistent. After the data is collected, these behavioural insights can be used to inform new strategies and enable firms to respond to such threats in real time.

"The cybercriminals of today manipulate people to give away their own details and make fraudulent transactions. On the surface, this means everything will match the bank's records, making traditional fraud detection controls defunct," says Mazor.

"The one element that gives them away is the change in the user's genuine behaviour – thus giving us critical clues of financial fraud. Modern behavioural biometrics monitors and analyses these behaviours continuously and in real time to protect financial institutions and consumers before they are impacted."

For more information about BioCatch's behavioural biometric solution, visit biocatch.com

BioCatch

Westend61 via Getty Images

of UK payments decision-makers have seen an increase in payment decline rate since the SCA rules were enforced

said that customers would wait only 1–2 minutes before walking away from a purchase because an SCA-compliant checkout process can be too long

said SCA rules need to go further to prevent fraud

Nuapay, 2022

AUTHENTICATION

Are new remote payment measures cutting fraud?

Entering a one-time password to complete an online transaction is now mandatory, so is secure customer authentication working? Or have fraudsters simply changed tactics?

Sean Hargrave

Anyone who has shopped online recently will be used to using a one-time password (OTP) or log onto their mobile banking app to approve a purchase.

This secure customer authentication (SCA) step became mandatory in March, as ecommerce providers were obliged to ensure customers prove their identity by proving something they know (a password) and using something they own (their mobile phone).

The measures were brought in because, according to figures from the banking and financial industries body, UK Finance, remote purchases accounted for four in five (79%) card fraud cases during 2021. By sending the legitimate customer a one-time password or asking them to log into a bank app, the hope is that fraud rates will drop.

It will not be known how well the new measures are working until the end of the year, when UK Finance will publish fraud figures for 2022. But Nationwide credited the technology with recording 2,000 fewer cases of fraud each month. Its research has shown that more than two in three customers, 68%, are happy to enter a texted passcode or, as the majority do, approve a payment in their banking app.

But not all companies within the industry are convinced. Tonia Luykx, VP at fraud detection business Sift, claims its figures show that, at the very least, criminals have simply changed tactics. Its network measures fraud across thousands of merchants and has seen a 41% rise in fraud attempts since SCA was introduced. This, she says, is mainly down to criminals changing tactics and using stolen card credentials on goods under the £30 limit at which SCA protection is mandatory.

"SCA is definitely a step in the right direction but we're seeing fraudsters adapt," she says.

"They're defrauding sites by making lots of fraudulent payment attempts that are under SCA's minimal payment level and then, for larger payments, they are taking over accounts and sent a password to complete a transaction."

Fraudsters take over accounts by tricking people into passing on their email address and password, typically through phishing, or duping a network into thinking a person is changing SIM cards and so needs messages sent to a new number. This new number is owned by a fraudster who then picks up any OTPs without the victim knowing.

> **SCA is definitely a step in the right direction but we're seeing fraudsters adapt**

Neil Downing, VP of products at TMT Analysis, reveals there has been an uplift in fraudsters using tactics such as a SIM-swap to circumvent SCA's protections. Without detection technology, this type of fraud can be difficult to spot because so many people are legitimately changing their mobile phone number that the deception continues until the victim spots unexpected charges on their accounts.

"As an industry we see exploits against SMS vulnerabilities are on the rise, either through SIM-swapping or SIM-jacking to intercept a message, or telephony-based social engineering fraud to trick the victim into divulging the SMS one-time passcode and circumvent the security," he explains.

"However, although the industry is seeing significant growth in attacks against SCA, the risk of fraud from a reliance on password-only security is substantially greater. The humble SMS OTP is better than no SCA by orders of magnitude."

While security businesses commonly agree SCA is a welcome step in the right direction, there are plenty of experts who will point out the extra 'friction' in making a payment is having a negative impact on ecommerce. When there is an extra step to go through, consumers may think again about an impulse purchase, and many may not have a phone at their side to approve a sale.

Research from open banking payments platform Nuapay reveals that 99% of merchants have seen at least a 5% rise in declined payments since SCA was introduced. The average rate of increase in payments not being completed is 37%. While this figure will include payments that were declined because of insufficient funds, Nuapay's CEO Brian Hanrahan believes that because this has always been the case, most of the rise is likely down to SCA. It is a welcome addition in the battle against fraud, he maintains, but it has had a major impact on retailers because of how it had to be implemented.

"The problem is that cards are decades old and they're being used online, so payment providers have to put sticking plaster on them, like texted one-time-passwords, to try to make them safer," he says.

"That's why we expect merchants will start using technology to allow direct payments from bank accounts because they have security built in, just by the person logging on."

The payments industry will not be able to say for sure whether SCA has reduced card-not-present fraud until the end of the year. It is fair to say that the tactics used to circumvent its measures were already in use to take over accounts to make fraudulent payments. They grew in popularity during the pandemic, as more people started to shop online. Many were new to digital channels and the phishing methods used by criminals, making account takeover far easier.

When 2022 fraud figures are released, industry experts believe they will likely show SCA has caused criminals to switch to lower-value fraud, meaning the number of cases may be up but individual sums involved will be down. For higher value fraud, criminals will likely continue to rely on phishing and social engineering tactics to trick people into passing on log-in details so that their online accounts can be taken over. As ever, technology can only do so much. The biggest risk in the security chain is often the customer.

Commercial feature

Trust in blockchains will unleash the power of crypto

Sophisticated blockchain analysis is enabling organisations and law enforcement agencies to work together to combat illicit activity, unlocking the true value of cryptocurrency for the masses

The last decade has brought enormous growth in the adoption of cryptocurrency, from individual consumers and investors to businesses and institutions. Beginning life primarily as an alternative currency based on digital blockchain technology, use cases have proliferated in more recent years, with a big variety of projects now actively using or planning to use the technology.

Blockchain is set to revolutionise how we live and transact, and transform a range of different industries, far beyond the sectors most in the spotlight right now, such as art and gaming. But such is life that whenever a powerful new innovation is developed to help bring about positive changes globally, there are people who also seek to exploit those powers for nefarious means.

Criminals use cryptocurrencies for the same reason that millions of people use them for legitimate purposes: they are instantaneous, cross-border and liquid. The 2022 Crypto Crime Report from Chainalysis shows cryptocurrency-based crime hit an all-time high in 2021 when illicit addresses received $14bn, up from $7.8bn in 2020 and $4.6bn in 2017.

With opportunities for significant rewards, cybercriminals are becoming increasingly sophisticated in their techniques, including new and unfamiliar technologies. Scams have long been the largest segment by transaction volume and represent a significant threat to trust in the space, robbing victims of $7.7bn worth of cryptocurrency in 2021 alone. Within this growing landscape, 'rug pulls' have emerged as the go-to technique of the decentralised finance (DeFi) ecosystem.

Rug pulls are where the developers of a cryptocurrency project abandon the token and take users' funds with them. They accounted for 37% of all cryptocurrency scam revenue in 2021, up from just 1% in 2020. Around $3.2bn worth of cryptocurrency was stolen in 2021, a 516% leap compared to 2020, with 72% of that stolen from DeFi protocols.

This is not surprising given the mammoth 912% growth in DeFi transaction volume in 2021, with the incredible returns on decentralised tokens like Shiba Inu encouraging many to speculate. It's easy for those with the right technical skills to create new DeFi tokens and get them listed on exchanges, even without a code audit to publicly confirm that the contract's governance rules are iron-clad and contain no mechanisms that would allow for the developers to make off with investors' funds. A lack of regulation has left people wide open to these scams.

However, the report by Chainalysis also reveals that while cryptocurrency crime is growing in volume, it is shrinking as an overall proportion of the cryptocurrency ecosystem. Transactions involving illicit addresses represented just 0.15% of cryptocurrency transaction volume in 2021, nearly 10 times lower than in 2017. This shows significant progress is now being made.

"Though this shrinking proportion is partly due to the rapidly growing rate of crypto adoption, it's also because law enforcement's ability to combat crypto-based crime has evolved too, with the tools at their disposal improving all the time," says Michael Gronager, co-founder and CEO of Chainalysis, whose cryptocurrency investigation and compliance solutions help law enforcement agencies, regulators and businesses as they work together to fight illicit cryptocurrency activity.

"Law enforcement agencies also not only have more and more resources, as well as experience, to handle cases involving cryptocurrencies, but they have been increasingly able to seize illicitly obtained cryptocurrency. In November 2021, the IRS Criminal Investigations announced it had seized over $3.5bn worth of cryptocurrency in 2021, all from non-tax investigations, representing 93% of all funds seized by the division during that time."

The ability to track and recover assets is crucial as it destroys the financial incentive to carry out further attacks. Other examples include $56m seized by the Department of Justice in a cryptocurrency scam investigation and $2.3m from the ransomware group behind the Colonial Pipeline attack.

Yet despite the clear progress, there is still a long way to go in fighting illicit cryptocurrency activity. Criminal abuse of cryptocurrency creates huge impediments for continued adoption of this revolutionary technology, heightens the likelihood of restrictions being imposed by governments, and, worst of all, victimises many innocent people around the world.

> **Our mission is to build trust in blockchains to promote more financial freedom with less risk**

One of the most common misconceptions about cryptocurrency is that it is totally anonymous and untraceable, when in fact the opposite is true: cryptocurrencies present unprecedented transparency. They are the first global payment systems outside of any organisation's control and their blockchains create public, permanent records of transactions. The challenge is that the public blockchain ledger is very difficult to interpret, driving a need for better blockchain analysis.

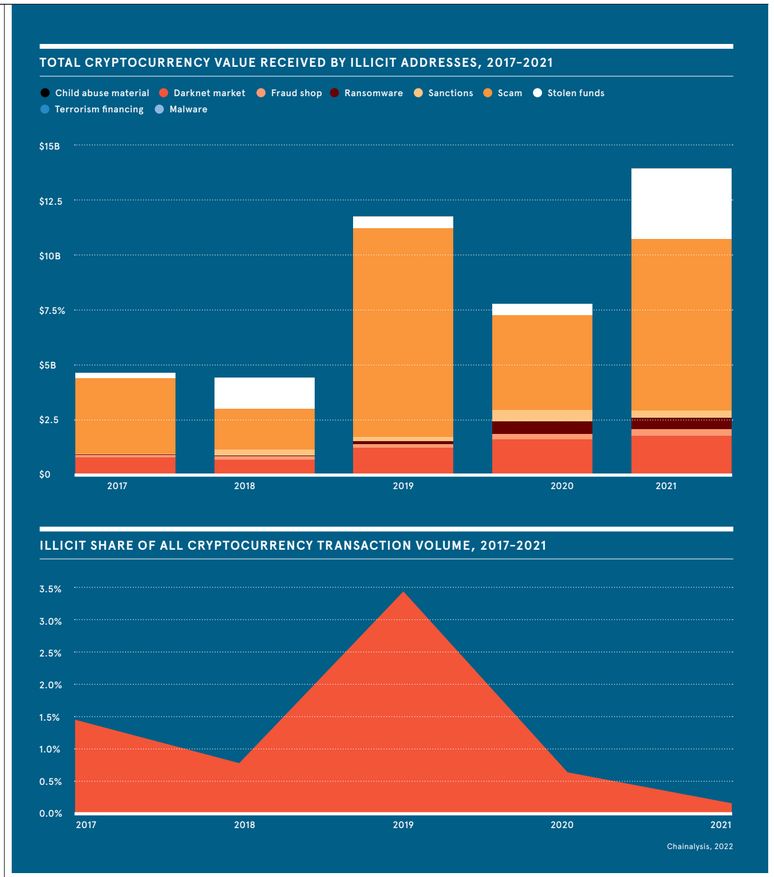
"That's where we come in," says Gronager. "At its core, Chainalysis is a data platform. Our data links cryptocurrency transactions with their real-world services." Chainalysis provides this data, as well as software, services and research, to government agencies, exchanges, financial institutions and insurance and cybersecurity companies in over 70 countries. Seeing which real-world entities transact with each other enables the organisations to work together to solve the world's most high-profile criminal cases and grow consumer access to cryptocurrency safely.

For example, Chanalysis can show that a given transaction took place between two different cryptocurrency exchanges, or between a cryptocurrency exchange and an illicit entity, such as a sanctioned individual or organisation. With blockchain analysis tools and KYC information, law enforcement can gain transparency into blockchain activity in ways not possible in traditional finance. Likewise, with transaction monitoring, cryptocurrency exchanges and financial institutions can flag high-risk activity and fulfil their regulatory obligations to then report them.

"By working from the same Chainalysis blockchain data, our public and private sector customers can collaborate more efficiently when investigating illicit activity," Gronager adds. "Our mission is to build trust in blockchains to promote more financial freedom with less risk. We believe transparency is critical to weeding out bad actors and building this trust in blockchains, which will ultimately pave the way for more mainstream adoption of transformative cryptocurrencies."

For more information, visit chainalysis.com

Chainalysis



NEOBANKS

Challenger banks challenged on fraud

Their growth has been explosive, and they've shaken up the world of banking – but there are growing concerns about how well challenger banks and fintech firms are handling fraud

Simon Brooke

Keen to increase competition and improve services for customers, the government and regulators in the UK and around the world have, over recent years, encouraged the growth of challenger banks. This drive has been successful – the market industry was valued at $20.4bn (£17.1bn) in 2019 and is projected to reach $471.0bn by 2027, a CAGR of 48.1% from 2020 to 2027, according to Allied Market Research.

But there are now growing concerns about how well some of these dynamic newcomers are managing financial crime fraud and anti-money laundering (AML). The UK's FCA undertook a review last year, which was published in April this year, and identified a noticeable increase in suspicious activity reports. The regulator is particularly concerned about the adequacy of checks carried out by challenger banks when onboarding new customers.

It highlights that, in some instances, these banks failed to adequately check their customers' income and occupation. The FCA also considered that some banks had underdeveloped or even entirely non-existent customer risk-assessment frameworks and that there was insufficient detail here.

"Challenger banks are an important part of the UK's retail banking offering," says Sarah Pritchard, executive director for markets at the FCA. "However, there cannot be a trade-off between quick and easy account opening and robust financial crime controls."

Fintech firms are in a similar position. In July, it was revealed that Monzo is being investigated by the FCA for possible AML breaches. "The prevention of financial crime is an issue that affects the entire banking industry and one which Monzo is taking extremely seriously," says the firm. "Over the past year, we have made major investments in our controls in this area as a priority and will continue to invest heavily in this part of the business."

> **There is an assumption that a substantial sum of money will inevitably be lost to fraud every year. It needn't be**

In July, it was revealed that challenger bank Monzo is being investigated by the FCA for possible AML breaches

Bloomberg/Contributor via Getty Images

The issue is not solely one that affects UK challengers. Last year, the German financial regulator BaFin slapped N26, an online bank, with more than 7 million customers in 24 markets, with a €4.25m (£3.59m) fine for delayed reports of suspicious activity in 2019 and 2020. In response, N26 said: "With the growing importance of ecommerce, we have taken numerous detailed measures and have also established structures and processes that meet the highest standards of financial crime prevention to address this pertinent global threat."

Can challenger banks continue to acquire customers at such a rapid rate and offer them a frictionless customer experience, while at the same time successfully managing growing threats from fraudsters and cybercriminals?

Part of the problem is that the speed of processes and interactions and the relative lack of bureaucracy that forms a key selling point for the challenger banks is just as appealing to fraudsters as it is to legitimate customers. Their lean, agile makeup means that they might lack the large anti-fraud and money laundering teams and extensive experience of the legacy banks. It remains to be seen whether, in the interest of addressing increased concerns surrounding fraud, these banks will be prepared and able to reject more new customer applications and possibly annoy existing customers by delaying and flagging up certain transactions.

"First and foremost, challenger banks must review their onboarding process to verify the identity of the customer and minimise the risk of money laundering," says Armen Najarian, chief identity officer at Outseer, an AI-driven anti-fraud firm. "While many challengers do exercise verification controls – like biometric technology – they must also provide adequate checks on their customers' income, occupation and background."

Najarian adds: "Machine learning has a big impact on power fraud prevention controls, giving challengers the same level of risk intelligence as a legacy bank.

"These solutions work in the background to verify customer identities and monitor transactions, credit card companies and banks. So challengers can detect and prevent fraud as well as comply with anti-money laundering regulations."

Given the novel, disruptive and rapidly evolving business models and systems employed by these institutions, does the law and the approach of regulators need to change here? "There is an assumption in the financial services industry that a substantial sum of money will inevitably be lost to fraud every year – but this need not be the case," says Najarian. "Regulators should do more to crack down on fraud, and this could mean having a minimum threshold for fraud prevention to ensure that banks have adequate protections in place to keep up with skyrocketing cases of fraudulent activity."

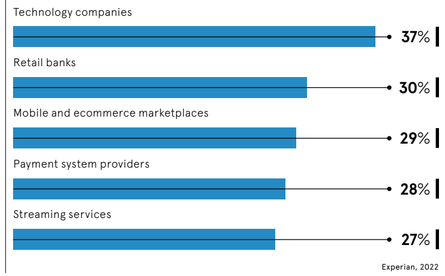
Challenger banks can take some comfort from the fact that the FCA's report is not entirely damning. It has found that: "Some challenger banks [are] mitigating fraud risk by incorporating additional monitoring for known fraud typologies at onboarding and as part of account monitoring. This included credit industry fraud avoidance system (Cifas) checking, as well as checks on customers using multiple devices to manage their accounts."

Their digital-first approach and sophisticated algorithms mean that challenger banks and fintech companies should be in a good position to start accumulating vast quantities of data quickly and effectively. This can be used, in conjunction with technologies such as AI and machine learning, to identify more actual and potential instances of fraud and money laundering and then to take action more quickly and effectively.

Meanwhile, as many longer-standing banks continue to struggle with legacy IT systems, there is the potential for the new generation of banks and financial institutions to innovate and lead the way in managing this increasingly important issue.

DO TECH-SAVVY CHALLENGERS HAVE AN EDGE WITH CUSTOMERS?

Percentage of UK consumers who say the following are their most trusted organisations for protecting them online



Experian, 2022

Commercial feature

Avoiding a financial crime horror show

How better workforce management tech can help financial institutions avoid the 'vampire' and 'zombie' compliance cases that can give them the regulatory jitters

Financial crime compliance costs are on the rise. As regulators impose tougher rules on financial institutions around know-your-customer (KYC) and anti-money laundering (AML) checks, firms are having to spend ever greater sums of money to keep pace. The projected cost of financial crime-related compliance was almost $214bn last year, according to a LexisNexis study—with roughly $40bn of that being spent in the UK alone.

The cost of non-compliance is clear. While KYC and AML-related fines fell globally last year, in the Europe, Middle East and Africa region, they more than tripled to $3.4bn, according to Fenergo. For example, Natwest was fined £264m for AML failures at the end of last year.

"Financial institutions have real challenges in meeting regulatory expectations," says Stuart Pugh, chief customer officer at ActiveOps, a workforce management software provider.

Against that backdrop, banks, insurance companies and other financial firms have been allocating a greater portion of their IT budgets to monitoring and detection technology to help flag suspicious transactions and criminal activity. What institutions sometimes then overlook is how to manage the ensuing workload.

"Most of the attention is on all of the software to detect things, but just detecting things is only half of the battle," says Pugh. "The other half, which is just as hard, is to actually have the capacity to process those transactions to meet your customer and regulatory expectations."

Traditionally, financial institutions have attempted to solve that problem by increasing the headcount of their compliance teams.

"They have been bringing in thousands and thousands of people to do that, but it isn't working," says Pugh. "These tend to be specialist roles with quite long accreditation and learning curves. So it's hard to just add people."

Given those specialists are in high demand, staff turnover is also frequent.

"It's harder to retain people and even when firms add more people, that doesn't translate into the improvements that they need to deliver," says Pugh. "So it has something of a feel of a limitless bucket—no matter how much resource you pour into this, you never actually achieve what you want to."

Part of the reason throwing more resources at the problem doesn't work is because existing processes are inefficient—which means adding more people simply results in more inefficiency.

Take a standard remediation case. Often the casework takes place over an extended period of time—90 days, say, for making a decision as to whether or not you are going to retain or close an account that has been flagged as high risk, says Pugh.

"That process will involve lots of interaction, you might potentially need information from the customer or other departments within the bank, and so for a lot of that time the case sits in a diary waiting for the next event to happen," says Pugh. "Now imagine you've got thousands of these cases, which are all following slightly different paths. And because they're all a bit different, they take different amounts of time to complete, which means they're all at different stages and being worked on by different people. That becomes a really hard challenge to plan so the right people are working on the right cases at the right time."

> **Using operational management tools can help give firms more confidence in predicting what they can deliver and more control over the process to ensure they do end up delivering**

At the moment, many financial firms try to manage this process manually by using spreadsheets to track the status of cases and what needs to happen next. Not only is that complex to maintain, it also increases the chances of certain cases being overlooked because processes are only designed to follow the trajectory of an average case.

"That doesn't really help you deal with the variation around that average," says Pugh. "Those variations are typically what we call 'vampire' and 'zombie' cases. Vampire cases are those that absorb a disproportionate amount of time—they get their fangs stuck in and just take much longer to resolve. Then at the other end of the scale you get the zombies—the cases that just wander aimlessly without anyone actually progressing them forward."

Vampire cases typically account for 30% of cases but can take up 70% of time.

Some financial institutions are solving this problem by turning to workforce management technology like ActiveOps so they can track how cases are progressing and flag when they deviate from the normal path a case should take. "That enables people to take action before it's too late," says Pugh.

By adopting technology to better allocate resources, firms can start to manage the process more efficiently.

"The first benefit is you get much more control over your cases and the second benefit is you know exactly how long each individual element of a case takes to be completed and you can then plan more accurately and have the right resources in place," says Pugh. "Because of the different variations with cases, you end up with different volumes of work within different teams and for different individuals. Unless you have a system that can pick that up, you end up with some individuals with too much work and others with too little."

This has knock-on benefits for customers and employees alike. For end customers, compliance issues can be resolved faster. In the case of onboarding and KYC checks, this reduces the risk that a potential new customer might switch to a competitor because they had to wait too long for their account to be approved. For staff, this technology can help reduce stress because compliance teams have more capacity and fewer time pressures.

"One bank we worked with had continually failed to meet their regulatory deadlines," says Pugh. "You can imagine the pressure those individuals were under and constantly failing to deliver what they had committed—and that was because they had no real underlying control in order to make a realistic commitment and then deliver against it. Using operational management tools can help give firms more confidence in predicting what they can deliver and more control over the process to ensure they do end up delivering."

By adopting tech to focus on the human element, financial firms can improve their financial crime compliance and avoid the zombie and vampire cases that can cause regulatory nightmares.

For more information please visit bit.ly/3aNIpdj

ACTIVEOPS

OCR Labs©

Fully Automated Identity Verification.
Anyone, Anywhere, Anytime.

16,000+ ID documents
in over **230** countries with
142 languages and typesets.

All powered by industry-leading
proprietary technology
developed in our labs.

100% users receive
a yes/no decision
in seconds

100% liveness
video fraud
assessment*

99.997%
face matching
accuracy*

Get your demo at www.ocrlabs.com/book-a-demo
or email hello@ocrlabs.com

www.ocrlabs.com

**We have our biometric algorithm tested by NIST & FIDO accredited biometric testing labs in accordance with ISO/IEC 17025:2017.*