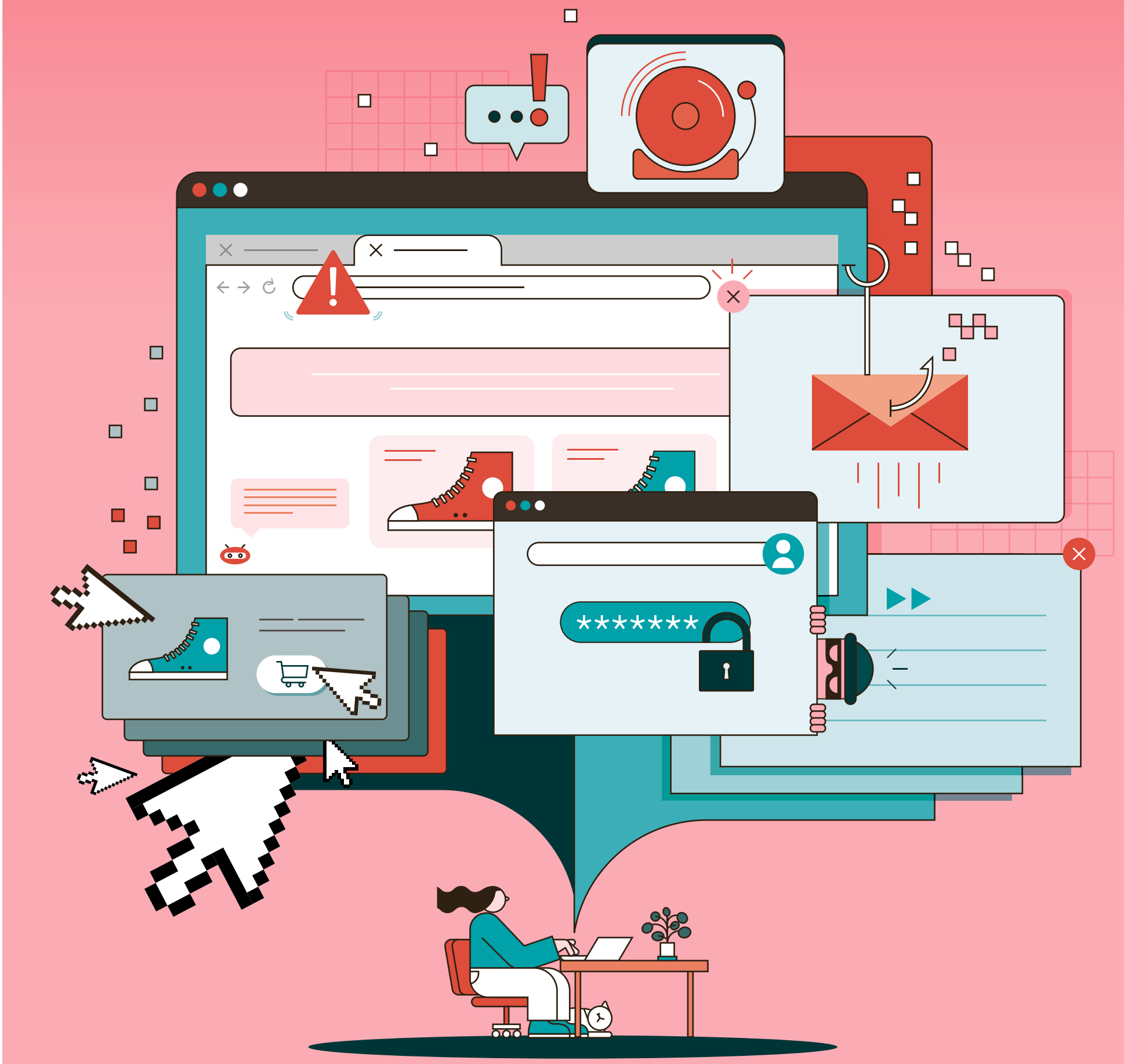
FIGHTING FRAUD



FIGHTING FRAUD

Distributed in THE TIMES

Contributors

Alison Coleman
A writer and editor working as a senior contributor at *Forbes*, with articles published in *The Guardian*.

Morag Cuddeford-Jones
A journalist, editor and broadcaster specialising in marketing and other aspects of business.

Sam Haddad
A journalist specialising in travel, with work published in *The Guardian*, *The Times* and *1843* magazine.

Christine Horton
A long-term contributor to IT titles such as *Channel Pro* and *MicroScope*, she writes about technology's impact on business.

Oliver Pickup
An award-winning journalist, specialising in technology, business and sport, who contributes to a wide range of publications.

Gareth Platt
A journalist and editor specialising in the future of work, with articles published in *Vice*, *The Independent* and the *IBTimes UK*.

raconteur reports

Publishing manager
Olly Eyre

Managing editor
Sarah Vizard

Deputy editor
Francesca Cassidy

Sub-editor
Gerrard Cowan

Head of production
Hannah Smallman

Design
Pip Burrows
Sara Gelfgren
Kellie Jerrard
Celina Lucey
Colm McDermott
Jack Woolrich
Sean Wyatt-Livesley

Illustration
Samuele Motta
Nita Saroglou

Art director
Joanna Bird

Design director
Tim Whitlock

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3877 3800 or email info@raconteur.net

Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at raconteur.net

@raconteur /raconteur.net @raconteur_london

raconteur.net /fighting-fraud-2021

INTERNAL FRAUD

Covid-19: the perfect storm for employee fraud

Organisations spend thousands of pounds each year protecting themselves from external fraudsters, but could the pandemic be increasing the threat from within?

Alison Coleman

Businesses have long contended with the risk of employee fraud, from false expense claims to data theft. But, for some experts, the Covid crisis could increase the danger.

The pandemic has driven a large-scale move to remote working. Some believe that this, when combined with the significant economic and social impact of the virus, could boost the conditions for internal fraud.

The risks were on stark display in a June 2020 survey by Crossland Employment Solicitors, which found that more than a third (34%) of UK employees had been asked by their boss to work while being furloughed by their company – an act of fraud under the coronavirus job-retention scheme.

In its 2020 report, the Association of Certified Fraud Examiners estimated that 5% of all revenue generated by organisations, or about £3.5tn globally, is lost every year to employee fraud. Its "fraud triangle" theory outlines the three components that lead to such behaviour: pressure or incentive, opportunity, and rationalisation.

The Covid crisis could have a dangerous impact in some or all of these areas. For example, personal financial pressure has been much in evidence as people grapple with an uncertain employment landscape, says Richard Hunt, founder and MD of Turnkey Consulting, a risk management consultancy.

"By December 2020, nearly 9 million people had to borrow more money because of the pandemic," he says.

Working from home also heightens the opportunity component, allowing unusual behaviour patterns to go unnoticed while removing the support that comes with regular face-to-face contact and check-ins. Furloughs and redundancies put extra pressure on remaining team members. Lay-offs not only increase people's workloads but also lead to changes in organisational processes and roles, which can in turn create potential conflicts in an employee's responsibilities.

"For instance, it may be that, instead of one person ordering goods and another receiving and paying for them, those two tasks now fall to one individual," Hunt says. "With the all-important segregation of duties removed, it's an easy step for this person to process payments for goods that they might have ordered themselves."

Thomas Barwick via Getty Images

And, for employees who are really struggling financially or facing some large one-off cost, rationalisation might come easy. It could be simple enough to justify fraudulent actions as short-term borrowing from an employer that will be repaid the following month. If the organisation fails to detect this, the employee might borrow more – without making a repayment.

Employee fraud isn't always the result of malicious intent. Sometimes it stems from desperation, incompetence, or even ignorance. But it always requires sensitive handling by business leaders. In the current climate, employers have shown greater sympathy to the pressures that employees are under. But these sympathies may not extend to those acting dishonestly, irrespective of any personal factors behind the behaviour.

The most effective approach is to focus on prevention, says Catherine Kerr, employment law partner at Primas Law. For most employees who feel driven to behave in a way that is inappropriate and out of character, there will be a build-up leading to a tipping point, she says.

"Employers who interact with their team and embrace mental wellbeing as part of their culture are more likely to identify these problems before they get out of hand," Kerr says. "An employee who feels supported is less likely to be pushed to act in a way that runs contrary to the employer's best interests."

While employee education can help to minimise the risk of external fraud, it is less likely to deter internal fraud. Employees who behave fraudulently will, in most cases, already understand the impact of their actions, says Kerr, who adds: "Organisations should focus on creating a supportive working environment in which an employee can look to their employer for help and understanding in challenging times."

There are steps that employers can take to minimise the internal fraud risk. For example, they could implement a zero-tolerance policy and confer accountability on everyone in the organisation. Regular evaluations and effective performance reviews should highlight a change in character, a decline in performance or evidence of financial difficulties, all of which can indicate potential problems.

Sometimes employees are coerced into fraud by their colleagues. In some cases, they may be aware that fraudulent activities are occurring but are afraid of reporting them. It's therefore important to introduce a confidential channel for whistleblowers, argues Andrew Durant, senior MD at FTI Consulting.

"If they don't feel safe, they won't step forward," he says. "Most frauds are detected by tip-offs. Employee education about the risk of fraud, and how fraudsters may target them or the business, is key to prevention and detection."

What should be done if an internal fraud comes to light? The first step is to mobilise the HR team, keeping the number of individuals involved to a minimum to avoid any unintended amplification of the problem. The suspect should then be interviewed, with the intention of putting the allegation to them and learning why they may have committed fraud.

This may eventually result in the termination of that person's employment, of course. But the process will also help the business to understand the underlying issues that led to the crime "and put in place controls to ensure that the situation is not repeated", says Iskander Fernandez, partner and fraud expert at BLM, a commercial law firm specialising in insurance risks.

34% of employees have been asked by their boss to work while being furloughed by their company

1 in 5 were asked to either cover someone else's job or to work for a company linked to their employer while on furlough

1 in 3 were asked to carry on with their normal job

Crossland Solicitors, 2020

DEEPFAKES

Fighting (fake) fire with fire: can deepfakes catch financial scammers?

While deepfake technology is often associated with fraud and manipulation, American Express is seeking to turn it back against the criminals

Gareth Platt

Most of us will have seen a deepfake video at one time or another, be it Donald Trump appearing on *Better Call Saul* or Tom Cruise performing magic tricks on TikTok.

The media coverage is often negative, telling us that deepfakes will enable deception on a massive scale. But at American Express the technology behind deepfakes is being used in the fight against fraud. By using hyper-realistic data to help train internal detection systems, the company's researchers believe that they can warn customers more accurately and minimise the number of unnecessary card stoppages.

It's certainly a bold strategy, not to mention a timely one. Global payment card fraud losses exceeded £20.6bn in 2019, according to *The Nilson Report*. It's almost certain that this figure increased last year. Various financial agencies have reported an uptick in fraud during the Covid crisis, attributing this to the growth in online shopping.

We've witnessed a dramatic rise in the sophistication of fraud tactics in recent years, driven by advances in digital tech. Fraudsters have never had more weapons in their arsenal. These range from phishing scams to botnets that can run card-testing schemes (where a fraudster "tests" a credit card number that they may have randomly generated, bought on the dark web or acquired using spyware) on an industrial scale. The advent of deepfake technology has enabled con artists to dupe victims into handing over their details by simulating the voices of relatives or company bosses.

In their attempts to stem the rising tide, many credit card companies are using machine learning (ML), a form of artificial intelligence in which computer systems improve automatically by adapting to the data they receive. Engineers feed reams of transaction data into the ML algorithm. With this data, the algorithm identifies patterns in fraudulent transactions – their size, their location, the time of day they take place – and submits this data to their fraud-prevention teams.

ML models offer three distinct advantages over conventional rules-based prevention strategies. First, they can incorporate a multitude of factors. Second, they can adapt to changing behaviour patterns. And third, they create fewer false positives, reducing the need for the card blockages that cause customers so much frustration. But there is one crucial caveat: they rely on realistic, high-quality data to identify patterns accurately.

This is where deepfake technology comes in. The technology is itself a form of ML, which relies on a pair of algorithms known as generative adversarial networks (GANs). The two algorithms are, in essence, trying to outsmart one another. One algorithm, the generator, creates the content, while its rival, the discriminator, looks for flaws. Accuracy and rigour are baked into the system.

> **Attackers are constantly working to find new exploits, with defenders often playing catch-up**

According to Dmitry Efimov, vice-president of ML research at Amex, GAN technology enables the company's data scientists to react rapidly to new types of fraud. By simulating spending patterns from genuine transactional data, the data science team can create vast amounts of records for their ML models without relying on real-life information.

"GAN is useful when we're not able to train a model because of a lack of data," Efimov says. "An immediate use case is our fraud model, because fraud patterns can change rapidly. Early detection is the key prevention. If we detect a pattern of fraud we've never seen before, we want to be able to protect our customers from it, so we want to train our model to detect these new patterns."

He continues: "To train the model you need lots of data – and we may have seen this new fraud pattern only a couple of times. That's why we started to explore whether GAN could help us to solve that problem by enabling us to use simulated data of that fraud pattern in order to train the [ML] models and improve their performance."

The project is still only at the research and experimentation stage. Although the GAN data has proved useful when the researchers haven't had massive swathes of historical spending data to work with (as is always the case when dealing with new customers), Efimov admits that all of the experiments completed so far have shown that "GAN-simulated data did not always improve the final models".

It remains to be seen whether GAN-based data will become a standard tool for fraud detection across the finance industry. Some commentators are sceptical, suggesting that there's a limit to the accuracy that these simulated records can offer.

"These arms-race dynamics are very challenging," says Henry Ajder, a freelance adviser on deepfakes, disinformation and the relationships between emerging technologies and society. "Attackers are constantly working to find new exploits, with defenders often playing catch-up in detecting deepfakes or suspicious bank transactions."

Generating synthetic data to train detection systems might give the latter a short-term edge, Ajder adds, but there's no guarantee how long that advantage will last. Still, he thinks there could be some benefits. "Think of anti-virus software: no company claims its software will catch every virus, although it does raise the barrier of entry by catching most examples that aren't on the cutting edge."

For their GANs to be truly useful, Amex's researchers will need to consider a full range of fraud scenarios in their data inputs. The sheer range of situations that could lead to fraud can be hard to replicate. As well as conventional card theft, for instance, the inputs must include cases in which the victim has been tricked into making the transaction.

"Humans are unpredictable," says Dr Edewede Oriwoh, an associate cybersecurity consultant with Quod Orbis. "Fixed, repeated patterns of behaviour, even when it comes to spending money, may not always appear. Patterns may change drastically depending on an individual's mood or recent events."

Amex will need highly varied methods "to ensure that its algorithmic model does not flag too many false positives", Oriwoh adds.

The scale of the challenge, then, is considerable. But some observers are optimistic about the project, viewing deepfakes as a genuine solution to fraud in the long term.

"If you're talking about recreating human faces or voices, there are still some telltale signs with deepfakes," says Leroy Terrelonge, a senior cyber risk analyst at Moody's Investors Service. "But, when you are dealing with a document that's essentially just numbers and text, I don't see what the barrier is."

Amex has data that potentially goes back all the way to the start of the company, Terrelonge notes. ML systems are powerful because they can recognise patterns far more quickly than humans.

"This seems like a very feasible use case for deepfakes," he says.

INTERVIEW

In the fight against fraud, Mastercard turns to AI

Ajay Bhalla, Mastercard's president of cyber and intelligence solutions, thinks innovations such as AI can tackle cybercrime – and help to save the planet

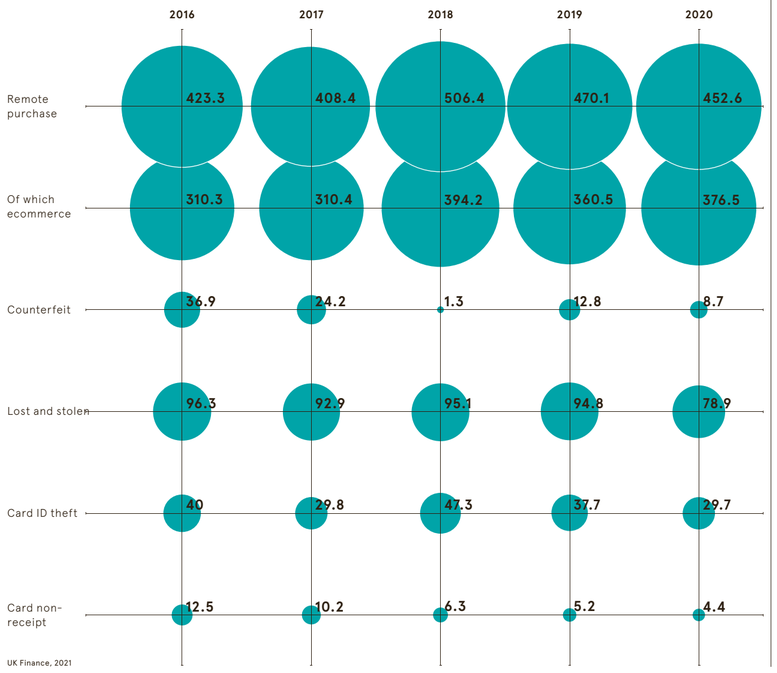
Oliver Pickup

The fight against fraud has always been a messy business, but it's become especially grisly in the digital age. To keep ahead of the cybercriminals, the financial services sector's investment in hi-tech countermeasures – particularly artificial intelligence – is paramount. So says Mastercard's president of cyber and intelligence solutions, Ajay Bhalla.

Since the start of the Covid crisis, cybercriminals have launched increasingly sophisticated attacks across a multitude of channels, taking advantage of heightened emotions and poor online security. About £1.26bn was lost to financial fraud in the UK in 2020, according to trade association UK Finance, while there was a 43% year-on-year increase in losses to internet banking fraud. It's estimated that the industry managed to prevent £1.6bn of fraud over the course of the year – the equivalent of £6.73 in every £10 of attempted fraud.

ARE BANKS GETTING BETTER AT CATCHING FRAUD OR NOT?

Card-related fraud losses over time (£m)



UK Finance, 2021

The landscape has changed rapidly over the past year, says Bhalla, citing factors such as the fast growth of online shopping and the emergence of digital solutions in the banking sector and beyond. These changes have broken down barriers to innovation, driving an unprecedented pace of change in the way we pay, bank and shop, says the executive who's responsible for deploying innovative technologies to ensure the security of 90 billion transactions each year.

"Against that backdrop, cybercrime is a $5.2tn annual problem that must be met head on," he says. "Standing still will mean effectively going backwards, as fraudsters are increasingly persistent, agile and well funded."

It's not only the growing number of transactions that's attracting the criminals' attentions, but also the diversity of opportunity, according to Bhalla, who has held various roles at Mastercard around the world since 1993.

"As the internet of things becomes ever more pervasive, so the attack surface grows," he says, noting that there will be 50 billion connected devices by 2025.

Given all these factors, AI will be essential to tackle cyber threats.

"AI is fundamental to our work in areas such as identity and ecommerce. We think of it as the new electricity, powering our society and driving forward progress," says the 55-year-old.

Mastercard has pioneered the application of AI in financial services through its worldwide network of research and development labs and AI innovation centres. Its AI-powered systems have prevented more than $30bn from being lost to fraud over the past two years.

In 2020, it opened an intelligence and cyber centre in Vancouver, aimed at accelerating innovation in AI and the internet of things. The company filed at least 40 AI-related patent applications last year, developing the biggest cyber risk assessment capability on the planet, according to Bhalla.

"We are constantly testing, adapting and improving algorithms to solve real challenges," he says.

Turning to examples of the company's work, Bhalla says that Mastercard has developed its ability to trace financial crime across its network – a world first. He also points to the recently launched enhanced contactless (Ecos) specifications, which use state-of-the-art security and privacy technology to make contactless payments resistant to attacks from quantum computers, using next-generation algorithms and cryptography.

"With Ecos, contactless payments still happen in less than half a second, but they are three million times harder to break," he says.

> **Cybercrime is a $5.2tn annual problem that must be met head on. Standing still will mean effectively going backwards**

£784m

was lost by UK banks and credit card companies to financial fraud involving payment cards, remote banking and cheques in 2020

£1.6bn

in potential losses to fraud were prevented by UK banks and card companies in 2020

UK Finance, 2021

Such innovations are transforming customers' interactions with financial services providers. For example, Mastercard has combined AI-powered technologies with biometrics – face, fingerprint and palm recognition – to identify legitimate account holders. These technologies recognise traits such as the way in which customers hold their phones or how fast they type – actions that can't easily be replicated by fraudsters.

"We see a future where biometrics don't just authenticate a payment; they *are* the payment, with consumers simply waving to pay," Bhalla says.

> **We see a future where biometrics don't just authenticate a payment; they *are* the payment, with consumers simply waving to pay**

Excited by developments in this area, he adds that Mastercard recently detected an attack that involved hundreds of devices attempting to log in from a phone that had reported itself as lying flat on its back. "Given the speed at which the credentials were typed, we knew it was unlikely it could be done with the phone flat on a surface," Bhalla says. "In this way, a sophisticated attack that looked otherwise legitimate was detected before any losses could occur."

Mastercard might have installed an impressive range of successful fraud-fighting measures, but wrong turns are a vital learning experience, Bhalla admits.

"If you don't test things to breaking point, you can be sure that their vulnerabilities will be discovered by criminals down the line," he says. "The need for trust in, and reliance on, Mastercard's services is far too important to take that risk, so rigorously testing solutions before they get anywhere near the end user is our standard operating procedure."

An avid golfer and oarsman, Bhalla volunteers as an executive in residence at the University of Oxford's Saïd Business School. The holder of a bachelor's degree in commerce from Delhi University and a master's degree in management from the University of Mumbai, he argues that Mastercard and others in the industry need to go back to basics and focus on customer experience. The company's leadership in standards has been core to earning and retaining the trust of consumers, he notes.

The technology may be evolving quickly, but one core principle remains unchanged, says Bhalla.

"Our business is based on trust, which is hard won and easily lost," he explains, adding that the correct operating processes and standards need to be in place from the outset, so that both customers and businesses can have confidence in the technology and trust that it will be both useful and secure.

"What has changed is the sharp focus now being placed on developing leading-edge solutions that prevent fraud and manage its impact," Bhalla says. "This is not surprising, given that the average cost of a single data breach has grown to £2.78m."

Providing a blueprint for business leaders, he strongly believes that "innovation must be good for people... and address their needs at the fundamental design stage of the systems we create."

Bhalla is using tech to fight fraud and improve financial inclusion, with Mastercard aiming to connect 1 billion people globally to the digital economy by 2025.

With much of his work focused on "protecting the world we have", his ambitions are broader still. Mindful that tackling climate change is especially high on the agenda for younger customers, Mastercard has launched a series of initiatives in the sustainability space. These include a new badge that identifies cards made more sustainably from recyclable, recycled, bio-sourced, chlorine-free, degradable or ocean plastics.

Much like the war on fraud, the campaign to restrict global warming is reaching a crucial stage. Thanks to the efforts of industry leaders such as Bhalla, the world stands a better chance of achieving a positive result on both fronts.

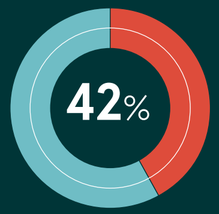
FIGHTING FRAUD DURING THE COVID CRISIS

The pandemic has changed various aspects of our lives and driven us online to shop, invest and date. Fraudsters have sought to take advantage of our new ways of living and working, playing on emotions and exploiting vulnerabilities – especially online. Unsurprisingly, the number of fraud and computer misuse offences surged in 2020 across the UK. But the statistics also show that methods of combating fraud are working

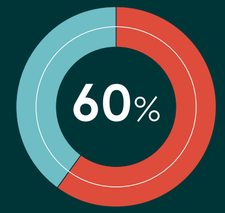
THE EVOLUTION OF CONSUMER BEHAVIOUR IN 2020

Lockdowns forced us to shift online to work, play and most things in between – and the fraudsters took advantage

LexisNexis, 2021



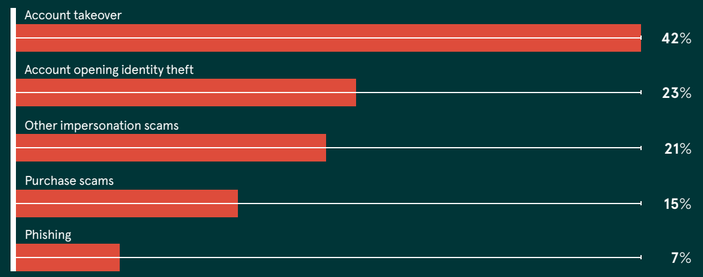
increase in digital transactions in 2020 (year on year)



of these transactions were mobile

TOP 5 BANKING SCAMS AROUND THE GLOBE

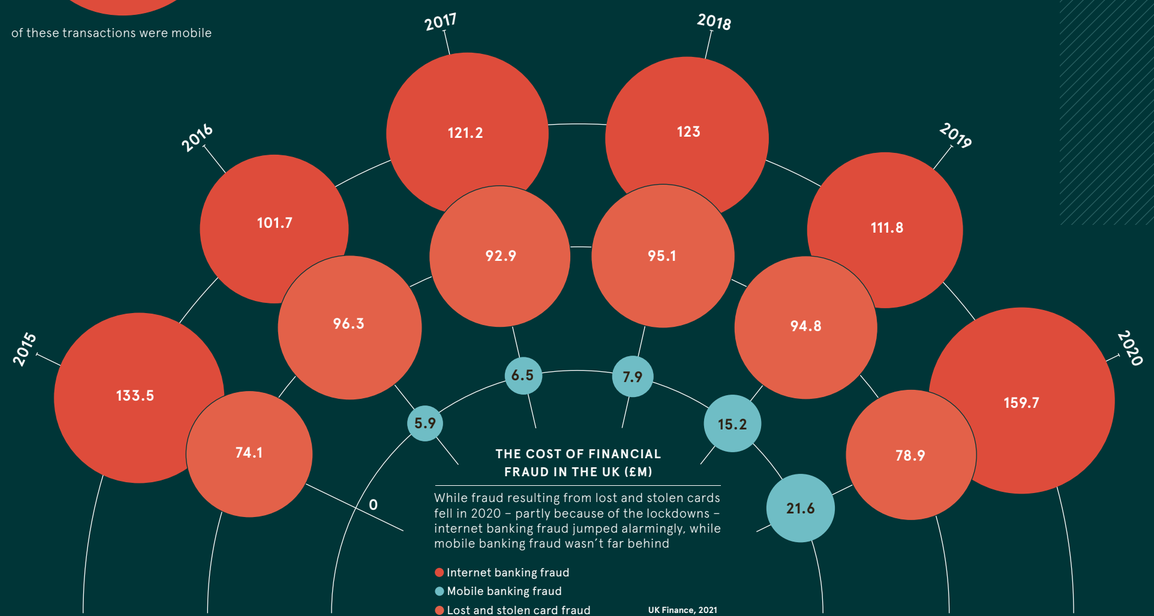
Percentage of total fraud attempts in 2020 committed using one or more of the following methods



Feedzai, 2021

THE COST OF FINANCIAL FRAUD IN THE UK (£M)

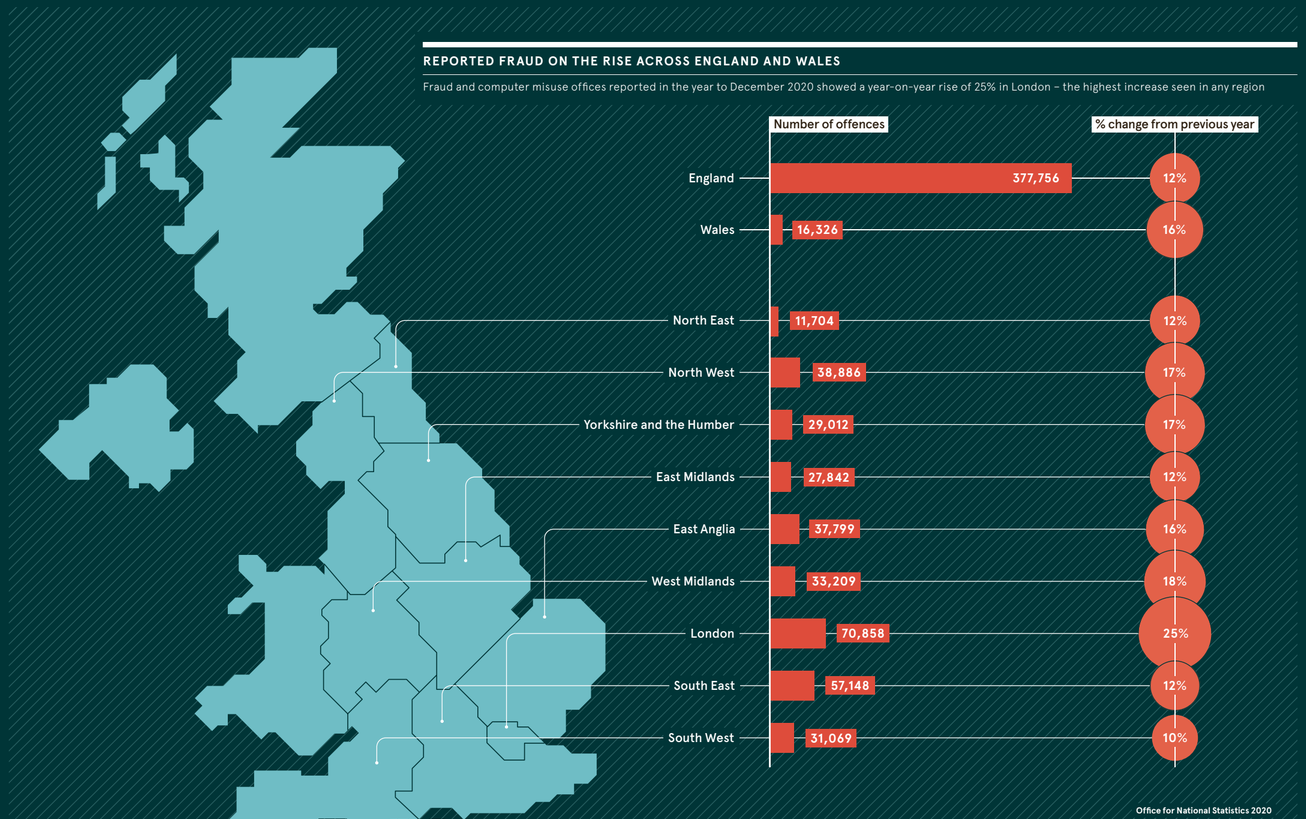
While fraud resulting from lost and stolen cards fell in 2020 – partly because of the lockdowns – internet banking fraud jumped alarmingly, while mobile banking fraud wasn't far behind



UK Finance, 2021

REPORTED FRAUD ON THE RISE ACROSS ENGLAND AND WALES

Fraud and computer misuse offices reported in the year to December 2020 showed a year-on-year rise of 25% in London – the highest increase seen in any region



Office for National Statistics 2020

LOSING OUT: FINANCIAL FRAUD LOSSES IN 2020 BY TYPE

Losses to financial fraud in the UK totalled £1.26bn last year. While online banking was used more readily, the fact that so few criminals sought to use cheques was a sign of the times

UK Finance, 2021

FIGHTING BACK: THE INDUSTRY'S RESPONSE

The foundations are in place to fight financial fraud, as illustrated by the figures from 2020, but more needs to be done – possibly with the government passing more legislation – to steal a march over the fraudsters

UK Finance, 2021

£45.3m

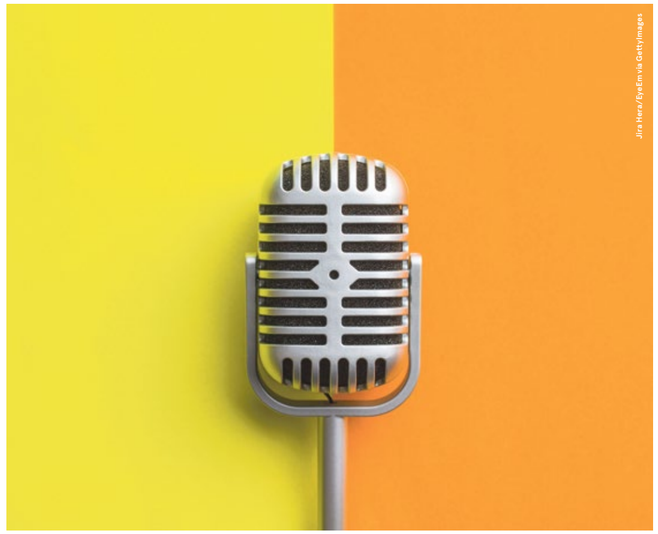
of fraud in UK was stopped in 2020 by the Banking Protocol

200

arrests were made because of the Banking Protocol in 2020

£147m

in losses were reimbursed in 2020 under the banking industry's voluntary code



Jira Nera / EyeEm via GettyImages

BIOMETRICS

Talking tough: banks boost security with voice ID

Voice ID technology saves banks and other enterprises millions of pounds every year, but is it a reliable identity marker in the fight against fraud?

Christine Horton

How safe is your voice as an identity marker? As biometric technology continues to make strides, opinion is split on whether voice tech is a blessing or a curse when it comes to fighting fraud.

Biometrics are based on physical or behavioural measurements such as the dimensions of someone's facial features or their hand gestures. Voice scans authenticate a person's identity based on modalities such as pitch and intensity, which are compared against a database of voice samples.

HSBC UK's voice ID technology prevented £249m-worth of fraud in 2020, according to the bank. Since its launch in 2016, the technology has prevented £981m of customers' money from falling into the hands of fraudsters, with the rate of attempted fraud down by 50% year on year as of May 2021.

"Telephone fraudsters may try to impersonate customers by stealing or guessing personal information to pass security checks, but replicating someone's voice is far more difficult," says David Callington, head of fraud at HSBC UK.

Voice ID detects whether the voice matches that on file for the customer "and therefore whether the caller is genuine", he explains. The bank's system allows it to make changes to different security settings – for example, limiting the number of attempts that can be made before manual authorisation is required. It regularly reviews and changes the system to enhance security.

NatWest also uses voice biometrics as an alternative to security mechanisms based on passwords to other static identifiers, which can be stolen or forgotten. The bank deploys a voice biometric solution from AI-based speech-recognition firm Nuance, which screens incoming calls and compares voice characteristics – including pitch, cadence and accent – against a digital library of voices associated with fraud against the bank. The software quickly flags suspicious calls and alerts the call-handlers to potential fraud attempts.

As well as a library of 'bad' voices, NatWest agents now have a whitelist of genuine customer voices that can be used for rapid authentication, without the need for customers to remember passwords and other identifying information.

Jason Costain, head of fraud prevention at NatWest, says the bank "can detect when we get a fraudulent voice coming in across our network as soon as it happens". Its technology is giving it a clear picture of what its customers sound like – and what criminal voices sound like, too.

"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 says.

But the rise of deepfake technology means that voice biometrics can be cloned and used to fraudulent ends. As the technology improves and becomes more widely available, the fraudsters will follow the money, says Susan Morrow, head of R&D at Avoco Secure, a digital identity specialist. The criminals will then create systems to exploit the technology using the same techniques.

While biometric technology is often viewed as the ultimate in authentication and verification, "this is a war of attrition. Voice biometrics – like any other tech – can only be seen as a risk-reduction method, not a cure," Morrow says. "Just as deepfakes for video have arisen, deepfakes for audio will increasingly be used for crimes that involve impersonation."

So how reliable is voice as a biometric marker and should banks and other enterprises rely on it? Security is not achieved by a single measure, especially when a system has multiple moving parts, as is the case with payments, Morrow argues.

"Voice biometrics is a useful measure, but it's only part of an overall system – and it will be exploited," she says. "As with any system, security measures need to be part of the checks and balances."

As customers part with their biometric data, there's also an issue of trust. Research by identity and authentication firm Callsign shows that only 38% of consumers feel comfortable using static biometrics, such as fingerprint ID or facial recognition, to confirm their identity.

"The problem with static biometrics is that it's intrusive and not privacy preserving," says Chris Stephens, head of solution engineering for Callsign in the UK, Europe and South Africa. "Static biometrics are also prone to inherent biases. Once they are compromised, there is nothing anyone can do to prevent attackers from getting in."

But a recent survey by GetApp, a company in the Gartner group, shows that younger customers seem more comfortable with the idea of using biometric technology such as voice scans compared with older generations. More than half of respondents from generation Z (born approximately from the mid-1990s to the early 2010s) said they had voluntarily shared biometric data with a private company, compared with only 29% of over-50s.

"These results should not come as a surprise, as a third of millennials and generation Z members have most probably had experience with this type of technology – for example, with chatbots and voice-activated devices such as Siri and Amazon Alexa," says Sonia Navarrete, senior content analyst at GetApp.

Organisations are clearly reaping the rewards of their investments in voice biometrics, particularly banks and other financial services providers. But it might be wise to view these systems as part of a broader, holistic approach to fighting fraud.

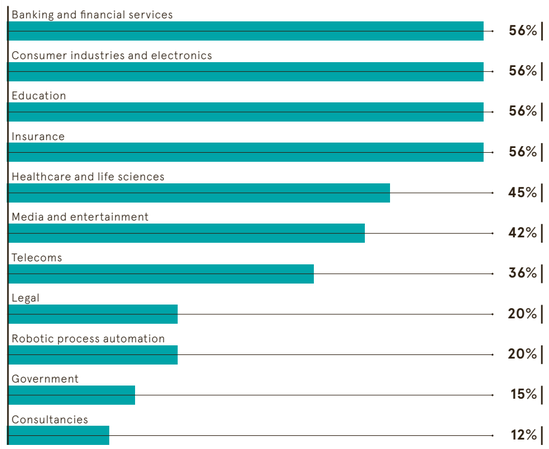
There are security limitations if businesses focus solely on voice technology, Stephens says. But, by layering in other verification requirements – for example, behavioural biometrics such as location or the way an individual uses a mouse – consumers can be allowed access to services such as online banking just as quickly, easily and securely.

"This also means that businesses hold only the information that's completely necessary," he says. "That helps to preserve privacy and build trust with customers."

> **Static biometrics are also prone to inherent biases. Once they are compromised, there is nothing anyone can do to prevent attackers from getting in**

WHERE VOICE ID IS SET TO MAKE A DIFFERENCE

Percentage of senior executives from each of the following industries who say they will increase their use and application of voice technology in the next three to five years worldwide



Speechmatics, 2021

Commercial feature

Human and artificial intelligence working together to fight payment fraud

In a rapidly evolving payments fraud landscape, it's important that merchants have strong fraud systems and machine intelligence behind them, but that should never mean sacrificing the human eye

The prevalence of fraud has risen rapidly as criminals have sought to take advantage of a unique pandemic-induced combination of financial and health threats which have made people more vulnerable to scams. The National Cyber Security Centre, the UK's cybersecurity agency, revealed last month that it has taken down more scams in the last year than in the previous three years combined, fuelled in particular by coronavirus and NHS-themed fraud attempts.

Though some may associate the rise of fraud with cybercriminals becoming more sophisticated, the reality is many old scams are among the most prevalent, with many people still falling for phishing attacks. Younger consumers have become well-versed on how to spot such scams, but the growth of digital activity among older generations, forced to shop online during the pandemic, has opened opportunities for fraudsters to target a far less tech-savvy demographic. A main entry point to scam consumers is when they are making a payment.

"Many consumers are starting to make payments online for the first time, going through the process of authorising a transaction via emails and messages. If they are not very cautious, they can be scammed into thinking similar-looking emails and text messages look legitimate," says Tom Pilling, chief risk officer at Trust Payments, a global payments technology company. "It is the perfect environment for fraudsters to scam people who are new to purchasing online.

"We definitely saw a big rise in fraudsters scamming people that traditionally don't purchase online. The modus operandi of a fraudster hasn't necessarily changed in a significant way. The methods fraudsters use to get through fraud engines and fraud transaction monitoring solutions have certainly evolved and improved, but when you look at the transaction itself and the information held within it, it is still the case that if it doesn't look right, it generally isn't right."

The more consumers fall for these types of scams, giving away their personal details, the more it also affects business owners and shop owners, many of whom have also been forced to embrace ecommerce during the pandemic. Unable to trade from their physical stores, merchants who previously had no online presence suddenly had to create a website or web shop very quickly to survive, while click and collect options also grew significantly.

While the ecommerce industry has raced ahead, payments companies have also had to be careful to reignite some of their early education programmes for merchants which were experiencing selling on digital channels for the first time. This has particularly been the case for smaller companies, which have needed educating on what they should be looking out for in terms of typical signs of fraud and scams, including, for instance, cardholders making repeat purchases in very short periods of time, average transaction value, or velocity-type checks.

"These things are quite standard to a lot of big merchants that have their own fraud teams in place but they're new to a lot of smaller merchants," says Pilling. "When you give merchants the education they need, they gain that additional layer of confidence. They can always consult with us to get advice about particular transactions, but you also see their confidence grow as they learn to make some of those decisions themselves. If an order looks too good to be true, it should spark caution with merchants. That human instinct is just as important as high-tech fraud tools."

Merchants, and indeed payment processors and acquirers, face the difficult challenge of not only trying to protect consumers from fraud but also balancing that with the need to provide a strong customer experience without making the payment process too cumbersome. Trust Payments, which powers online payments for some of the world's most well-established, as well as emerging, companies, has designed intelligent omnichannel payment solutions that monitor transactions for fraud while helping merchants grow, by ensuring the customer experience is seamless and convenient.

> **We continue to learn everyday with the volume of transactions we process online**

Trust Payments is dedicated to making as many decisions for merchants as possible with the smallest impact on merchant transaction authorisation versus decline. While committed to removing false positives, it is also focused on ensuring all the good transactions flow through without disruption. That means using real-time monitoring to look at different verticals, trends and types of transactions to determine what is good and what is bad. Those that sit in the middle, as potentially suspicious, will then be reviewed by a member of its fraud analyst team.

That balance is crucial. Though it's important for acquirers to be supporting merchants with sophisticated, machine learning-powered transaction monitoring systems, it's also vital that a human eye is maintained, both from fraud analysts working for the acquirer and also from the instincts of merchants, who often know the behaviours of their customers better than anybody.

"A lot of it is about learning," says Pilling. "We continue to learn every day with the volume of transactions we process online. And with that we're able to then also look at historical data to determine how we need to adjust our own rules so that we get that nice balance of good transactions, bad transactions and those transactions that sit in the middle that need further follow up and analyses. While our systems are really sophisticated from that respect, having that bit in the middle and the human side of things is key to the way we do our own analyses and educate merchants as to the type of transactions that they should be looking out for as well.

"There's absolutely no doubt that ecommerce is a growth area, but we're also supporting other emerging verticals. As well as our own in-house fraud solutions, we partner with different companies to provide a unique overall perspective of analysis. We look at those third parties that can do website analysis, for instance, our crypto blockchain analysis, to help create a really unique picture of transactions in the future. However, we must never forget that humans have that natural instinct, more so than machines, to know if it doesn't look right, it probably isn't."

For more information, visit trustpayments.com

TRUST PAYMENTS

CYBERCRIME

Ransomware: fighting a crime without borders

Ransomware attacks are tough to police, thanks to their global nature and use of cryptocurrency. Some experts are calling for stronger rules on cybersecurity

Sam Haddad

Two or three times a week, cybersecurity expert Jason Hart receives a call from a business that has been hit by ransomware attack.

The lucrative crime is committed by hackers who break into a firm's computer system and encrypt the data it holds, which they will release only once a fee is paid. It's hard to police, with ransoms paid in anonymous and unregulated cryptocurrencies. Public services are frequently targeted – one of Hart's recent requests for help came from a school.

The crooks can be anywhere in the world, operating across borders, says Hart, a former ethical hacker who's the co-founder and CEO of cybersecurity firm Fresh Security.

"They can be in El Salvador, hacked into a company in America, using a proxy back into Peru then across to Spain via Korea. They could be anywhere."

Ransomware made global headlines in May 2021, when a Russian hacker group called DarkSide forced the closure of the Colonial Pipeline, a fuel supply network that covers much of the eastern side of the US. But many ransomware attacks target low-profile small and medium-sized businesses, often going unreported.

The crime is seizing attention at the highest levels. "Ransomware is quickly becoming a national emergency," Brandon Wales, acting head of the US Cybersecurity and Infrastructure Security Agency, told a Senate hearing in late 2020. An EU report from the same year found that ransomware attacks grew 365% in 2019, inflicting about £8.7bn of losses on businesses.

To complicate matters further, cybercriminals in countries such as North Korea, Iran and Russia sometimes operate with the blessing and even encouragement of their governments, mounting attacks that can cause huge problems for other nations. The WannaCry 2.0 ransomware attack in 2017 – for which North Korea was blamed – seriously disrupted the UK's National Health Service and the state railway network of Germany. Tellingly, DarkSide's code automatically avoids encrypting a computer system that uses Russian as its language.

"There are non-democratic states that invest a lot of money in these types of cyberattacks," says Dr Lena Connolly, assistant professor in information security at Zayed University in Dubai. "They are very sophisticated – and you can imagine the resources they have to hand. But, if there is no evidence and no admission, how can another government respond?"

> **If the basics of cybersecurity were actually dealt with, ransomware attacks wouldn't be so prolific**

There have been some governmental responses, although not many. In February 2021, French and Ukrainian prosecutors arrested a gang that had rented out powerful ransomware for other cybercriminals, for instance. And in April, the US government sanctioned several Russian entities, citing "disruptive ransomware attacks and phishing campaigns" against Ukraine, the US, Georgia and France.

China recently blocked several crypto-related accounts on Weibo as part of a broader crackdown on cryptocurrency and its links to criminality. So is banning cryptocurrency the answer to ransomware? Connolly doesn't think so.

"Before cryptocurrency, criminals had other means to commit crime," she says. "Cryptocurrency is a wonderful technology. It can open up so many opportunities for businesses and individuals. It feels narrow-minded to ban it. The internet is also a facilitator, but we don't talk about banning that."

She adds that cryptocurrencies could be regulated – as is starting to occur in Switzerland.

For Connolly, ransomware is prevalent because it's relatively low risk and highly profitable for criminals. Some ransomware groups are so flush that they run call centres to talk victims through the extortion process. Recernt research by cybersecurity firm Kaspersky has found that more than half of ransomware victims are paying ransoms, but only just over a quarter are getting all their data back.

"Victims are paying up," Connolly says. "Law enforcement agencies advise them not to, but situations are difficult sometimes. Ransomware doesn't just encrypt data; it steals it, so you have the fear of incrimination, embarrassment and the loss of intellectual property. We're humans with emotions, which affect our decisions."

One promising state-level initiative is the new Ransomware Task Force, a US-led coalition between government agencies such as the National Cyber Security Centre in the UK and software companies, cybersecurity vendors, academics and not-for-profit bodies. It aims to find policy solutions, such as incentivising victims not to pay ransoms by covering the costs of their system recovery needs and subsidising back-ups.

The most important step that governments could take would be to force companies to protect their data through regulation, according to Hart, who doesn't advise victims to pay hackers.

He believes that, although there has been a lot of noise around ransomware, it's only a symptom of a far bigger problem. "If the basics of cybersecurity were actually dealt with, ransomware attacks wouldn't be so prolific," he argues.

Hart has worked with some of the world's largest organisations, as well as smaller companies. Only about 1% have conducted a proper risk assessment regarding their data. "The first thing I say to them is: 'What are you trying to protect?' And they don't know," he says.

Companies might think they are safe because they have a firewall, a secure virtual private network and anti-virus software. But this can result in a "vanilla blanket of security across the whole organisation", Hart says, when there could be specific data that is at greater risk.

He encourages clients to "think like a hacker" and look at all the types of data they have, providing extra protection to the material that needs it, including limits to access within the organisation.

For example, a school might hold sensitive data that could be damaging to a student and their family if released to the outside world. A ransom attack could also compromise the integrity of certain academic data if it aimed to, say, change students' grades.

£8.7bn
estimated to be paid in ransoms in 2019

45%
of victims paid the ransom

365%
increase in detections in businesses

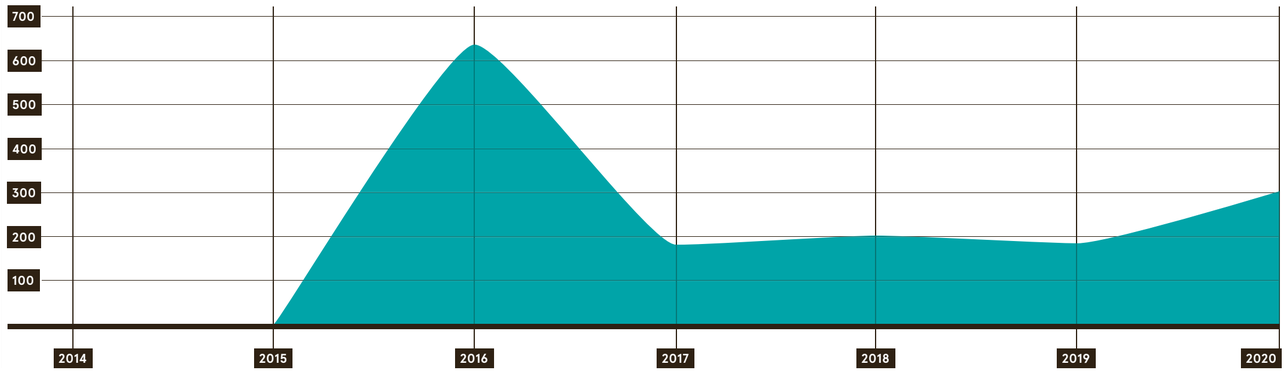
28%
of security incidents were attributed to malware

European Union Agency for Cybersecurity, 2020

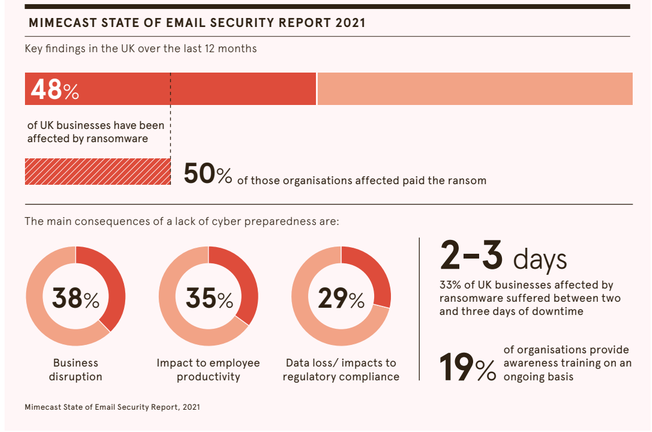
ARE WE GETTING BETTER AT FIGHTING CYBERCRIME?

The number of ransomware attacks each year from 2014 to 2020 (millions)

SonicWall, 2021



Commercial feature



Why cyber security is everyone's business

Meeting the sheer volume and variety of threats businesses face daily can seem daunting, but simple steps improve your cyber resilience

The accelerated shift to online over the past 18 months has been a boon to many businesses and a lifesaver for some. But with the rise in online activity has come an equivalent increase in cybercrime. With staff having to rapidly adopt remote working, the lines between business and personal technologies have become blurred, weakening organisations' defences against the criminals. Attacks are varied and more sophisticated, ranging from malware and ransomware attacks to denial of service, domain spoofing and more.

"The preeminent threat, for at least the last year, has been ransomware," explains Mimecast's head of risk & resilience, e-crime cyber & investigation, Carl Wearn, describing a common attack where companies' systems are infiltrated and taken over by criminals who either shut down access or threaten to leak customer data unless paid a ransom – hence the name. The common perception of such criminals is a lone wolf, hacker or organisation with a political aim. The reality is much more ordinary. "The vast majority of ransomware attacks are opportunistic. It's lucrative for the criminals and victims are reluctant to report it because of the impact on their brand reputation."

But while the temptation might be to keep quiet and pay up, the threat to business and brand reputation doesn't end there. "Not reporting it is a hindrance for law enforcement. In many cases, they are able to get some, or even all, of the money back from the criminals. But companies fear the resulting publicity will mean they are either open to a copycat attack, or that they might lose their customers' trust from having fallen victim in the first place," Wearn explains.

Despite the growing number of insurance products claiming to protect against cybercrime, payouts are by no means a given and, in some cases, the presence of coverage may actually encourage an attack. In most instances, companies should take simple steps to protect themselves against cyberthreats.

Cloud storage has become increasingly popular over the years and for good reason – it's flexible, comparatively inexpensive and generally secure. But it's important to be security conscious with any cloud storage or backups, as these can be targeted for encryption, like anything else.

Organisations should make sure they have fallback email and archive capabilities. "With a solution in place, even following an attack, you can continue to use email and carry on once you have restored from backup. Without that backup, once an attack has happened, it's clearly too late," Wearn warns.

Then it comes down to basic IT hygiene. Companies can take very basic steps to protect their systems. A strong password regime, for example, where regular changes are enforced, is the first line of defence. Awareness training is a key element here as employees must be aware of their role in cybersecurity. Multifactor authentication as standard is an additional layer of protection that is simple to institute. Segmenting networks so they can be cut off from the rest of the system and quarantined can prevent attacks escalating.

Company culture also plays an important part. "It's not uncommon for senior staff to insist on having admin access to applications but this just introduces more weakness into the system," Wearn suggests. "Resist the temptation to bow to job titles and restrict access to only the people who know how to keep those systems safe." Businesses should be insisting on a separation between work devices and technology for personal use.

Increasingly, organisations are looking to leverage cyber intelligence across multiple systems. Mimecast uses specific APIs to help systems collaborate and share knowledge of threats across the security ecosystem. Ultimately, resisting malicious actors online comes down to a joint effort between business, employees, specialist vendors and consultants and law enforcement.

Wearn concludes: "Take the time to research and collaborate with cybersecurity experts and select 'best of breed' solutions to provide layered security that suits your needs best. Implement awareness training for all users. Security is everyone's responsibility, particularly now we are all embracing a hybrid working model."

For more information visit www.mimecast.com/times

mimecast

Photographer: Basak Gurbuz Dermanvia GettyImages

ADVERTISING

Winning the race against ad fraud

Businesses need to treat ad fraud as another cyber threat, taking a risk management approach to the problem

Morag Cuddeford-Jones

Ad fraud is big business for criminals – and a growing problem for companies.

Fraudsters can adopt a range of scams (see panel, opposite page) aimed at cheating advertisers out of their money, from selling adverts on fake websites to concealing the true origins of online clicks. According to *Forbes*, the average perpetrator will make anywhere from £3.6m to £14.4m a year, though it notes that "ad fraud costs are all over the map".

The cost isn't just felt in the ad budget. The losses can occur all along the chain.

"If $100,000 worth of adverts is unseen, that could mean an overall loss in revenue of $1m," explains Dr Roberto Cavazos, executive in residence at the University of Baltimore's Department of Information Systems and Decision Science. Every dollar lost is potentially a multiple in lost sales, he says, adding that the scale of the crime "even affects economic stability".

If the impact of ad fraud is hard to estimate, imagine how hard it is to track and stop. Cavazos observes that there is a race occurring between the criminals and the companies developing countermeasures, with the danger always evolving. Indeed, it's hard to know which form of ad fraud is most concerning, he says, with the answer hinging on an advertiser's particular activities, among other factors.

Tina Lakhani, head of ad tech at trade body the Internet Advertising Bureau UK (IAB), agrees. She says that there's a range of technologies available to help monitor and mitigate ad fraud. The challenge lies in "evaluating different technologies out there, knowing which ones to work with and where to start".

The IAB has been creating industry standards for such technologies, along with bodies such as the Trustworthy Accountability Group, helping to assure buyers that their security providers have been independently audited.

Cavazos thinks there's potential to include internet fraud within international agreements in digital security. But it may be some time before the structure of the online ad industry evolves to be able to mount a stronger defence against the fraudsters, he says.

To determine the appropriate solution for a particular company, Lakhani encourages marketing and technology leaders to talk to their vendors. "You have to take an informed view, so ask them direct questions about how they protect against specific areas. Collaborate with them to understand how their technologies work and what their methods are. They may be able to teach you about fraud tactics you hadn't even been looking out for."

Sophisticated technological solutions aren't an option for everyone, Cavazos notes, particularly small and medium-sized enterprises or perhaps companies in developing nations. But Lakhani stresses that many fraud-mitigation vendors' business models are based on a percentage of overall ad expenditure, rather than a flat fee or the number of incidents they attempt to detect. Despite this, she acknowledges a degree of frustration among companies that see their investments in fraud detection as a kind of "tech tax" or "leaky bucket".

Companies' efforts to fight online fraud should be viewed as a form of cybersecurity, Cavazos says.

"Everyone imagines that someone in a hoodie is trying to undermine the treasury. But what happens is that a company spending $1m on advertising is actually getting $750,000," while also taking a hit to brand recognition, potential sales and more, he says.

> **"If $100,000 worth of adverts is unseen, that could mean an overall loss in revenue of $1m**

Lakhani adds that such solutions are important from a reputational perspective, adding value in areas of concern for advertisers, such as verifying environments and the content that ads appear against.

"These are all important considerations, especially if you're making a substantial investment in online advertising," she says.

THE GLOBAL COST OF AD FRAUD

Economic losses owing to digital ad fraud in selected countries in 2020 ($bn)

Cheq, 2021

Five key types of ad fraud

1 Domain spoofing

Domain spoofing can cost advertisers up to $1m in lost revenue each month according to anti-fraud company Anura. It occurs when firms – and the agencies they rely on – believe that they're advertising on a legitimate website when it's actually fake. The fraudsters create a plausible web address to attract advertisers that would probably never choose to use them, either because their audiences are small or because their editorial content is inappropriate. At best, it wastes your advertising budget. At worst, it aligns your brand with criminality or even terrorism.

2 Ad stacking

Particularly common on mobile, ad stacking is a simple but effective way for fraudsters to fill their coffers. The consumer sees a single ad that they may click on. But beneath that ad can be many more. Although unseen by the end user, they each trigger a charge. The ads have loaded correctly and appear to have been clicked, skewing the advertiser's cost per click or "cost per mille", the amount it pays per 1,000 views of the advert. These costs are justified only if a certain number of potential customers go on to buy the advertised offering. But, of course, those who have never seen the ad won't purchase, leaving the victim wondering why so many people are clicking yet so few are buying.

3 Ad click and bot fraud

This doubles down on the sort of fraud seen in domain spoofing, where advertisers mistakenly believe their ads are on a genuine site. By adding click fraud to the mix, scammers can further increase their revenues. Click fraud uses either bots or low-paid humans in a so-called click farm to generate huge amounts of clicks on adverts, which all use up ad budget that goes to the fraudster.

4 Click injection

This occures where cybercriminals put malware on users' devices via downloads of junk apps (an example could be apps created for a single fad, such as face-changer apps), which are cheap and easy to create. The malware generates clicks on ads – which could be run on platforms such as Facebook Network, for instance – which inflates expenditure and creates revenue for the developers. One firm investigated two such junk apps that had generated 3,061 requests for an ad and 169 successful clicks on a mobile while it was in sleep mode for 24 hours.

5 Geo masking

The world wide web is just that – worldwide. But an advertiser might not want to sell to certain countries for a range of reasons – the high cost of shipping, for example. Companies only want to pay for high-quality leads in the countries they want to target, so clicks from those countries usually come at a premium. Geo masking hides the origin of clicks, making it look like they all come from premium locations, inflating the overall cost of ads without delivering serviceable leads.

Want the power of print media combined with best in class lead generation?

Raconteur's new campaign product suite gives marketers the best of both worlds.

Email enquiries@raconteur.net to plan your campaign now.

RACONTEUR