FIGHTING FRAUD

Born in the Cloud, Raised by A.I.

The World's Most Advanced Fraud Prevention Platform

▶ One Platform, 100's of Solutions

Unify your proprietary and 3rd party data within a single integration.

▶ Global Consortium Data

Fuel your customer insights with billions of transactions and outcomes.

▶ Custom A.I. Models

Leverage deep learning algorithms and dedicated data science teams.

▶ Rapid Deployment

Accelerate your time to impact with agile, modular architecture.

REAL-TIME ENTERPRISE FRAUD DETECTION, CASE MANAGEMENT, AND ANALYTICS

Schedule a free 30-minute fraud prevention consultation.

Fraud.net

Fraud.net/times | sales@fraud.net | 866.971.2030

FIGHTING FRAUD

Distributed in
THE TIMES

Published in association with
Money 20/20 USA
OCTOBER 27-30, 2019

raconteur reports

Publishing manager
Hannah Smallman

Associate editor
Peter Archer

Deputy editor
Francesca Cassidy

Managing editor
Benjamin Chiou

Digital content executive
Taryn Brickner

Head of production
Justyna O'Connell

Design
Joanna Bird
Sara Gelfgren
Kellie Jerrard
Harry Lewis-Irlam
Celina Lucey
Colm McDermott
Samuele Motta
Jack Woolrich

Head of design
Tim Whitlock

BREXIT

Risks rise as UK enters uncharted territory

Fraud flourishes amid uncertainty, raising concerns for businesses staring down the barrel of Brexit

Michelle Perry

Fraudsters thrive in disorder and chaos. Where there is disruption, criminals will wheedle their way in to take advantage of the confusion. A prime example is the recent collapse of 178-year-old tour operator Thomas Cook and ensuing potential for business fraud. Just days after the firm failed, banks and other financial services providers were warning customers about scammers.

That was just one company collapse. On October 31, the UK is set to leave the European Union, which means an almost 50-year multi-layered relationship would be unravelled. In this unravelling and the resulting confusion, fraudsters will look to prey on vulnerable businesses.

"Initially, Brexit will present quite a threat. If we leave the EU, and even if we don't, the uncertainty that goes along with it puts us in uncharted territory," says Marc McAuley, counter fraud services lead at the Chartered Institute of Public Finance and Accountancy (CIPFA).

"We don't know what rules or regulations will be imposed on the UK public sector and UK business. But the rules will be certainly changing. And anytime there's uncertainty or change it creates a threat for us and an opportunity for fraudsters to exploit our weaknesses, the ambiguity and uncertainty."

Roy Waligora, head of investigations and corporate forensics at KPMG, adds: "Brexit will affect us in many different ways. Overall though, it would be imprudent to assume some level of disruption, and potentially chaos, won't happen.

"Fraudsters are very agile and that does, to our mind, create the opportunity and environment for fraud. Fraud in general in the UK is a sizeable problem and a challenge both for corporates to deal with and also law enforcement."

It is not, however, straightforward to pin down a concrete figure for the total value of business fraud in the UK, but it is clear fraud is a problem that is on the rise. The National Crime Agency (NCA) puts the total cost of fraud in England and Wales at £190 billion. The private sector is impacted the most, losing around £140 billion, according to the NCA's estimates. The estimated cost to the public sector is around £49 billion, while individuals lose around £7 billion.


Frederick Tubiermont/Unsplash

Amid the Brexit confusion there are certain areas where fraudsters may seek to take advantage of businesses, according to KPMG. These areas concern changes to the legal and regulatory landscape, business investment, tax and changes to the location of operations.

Many EU directives have been incorporated into UK law, but others have not. CIPFA's Mr McAuley says this uncertainty over which rules the UK will keep and which it will not will create a gap that criminals can exploit.

"We've incorporated the EU's General Data Protection Regulation into UK law, but there are other rules and regulations set by Europe that if all of a sudden we withdraw, what happens to those? Do we continue to abide by those rules or will business and the public sector deviate from them because they are no longer UK law? These are the areas that will create confusion and uncertainty. I believe there will be a spike in fraud intent," he says.

Worryingly though, the first wave of fraudsters seeking to exploit loopholes and confusion over legal and regulatory changes are likely to be industry insiders, KPMG says. Businesses may misrepresent their levels of access rights, tax benefits or central grant funding to secure investment, or business restructuring leading to job losses may cause a rise in business fraud.

When it comes to cyber-fraud attacks, it is less relevant whether the UK is in or out of the EU. Cyber-fraudsters operate on an international level from diverse locations around the globe. Arbitrary geographical borders are an irrelevance to international fraudsters.

"There's some assurance and confidence in our enforcement, but it's the unknown – what the attack will look like – and the level and methodology of it, as well as whether or not we are ready to cope with it," says Mr McAuley.

And here's the rub: cross-border cyberattacks are increasingly dealt with by cross-border counter fraud teams working collaboratively around the world. There is a risk that Brexit could impact information-sharing among law enforcement agencies. Overseas arrest warrants could also be affected.

One advantage to leaving the EU single market, however, could be a fall in the incidence of carousel fraud, also known as missing trader fraud, in the UK. Carousel fraud is where criminals import goods VAT-free from other countries, then sell the goods to domestic buyers, charging them VAT. The sellers subsequently disappear without paying the tax to the government.

It will not reduce this kind of fraud overall, but the VAT scam will be displaced to outside the UK. However, just as quickly as one tax fraud fades, another is likely to take its place.

A further opportunity for business would be to embrace the upheaval of leaving the EU and use it as a chance to review all policies and procedures in the supply chain, knowing your business partners and other aspects of a business vulnerable to fraud.

It is unlikely fraud prevention will ever eradicate business fraud. And as new technologies bring us untold benefits, they also aid organised crime to devise new ways of defrauding businesses.

Cybercrime is clearly set to grow, so governments and business leaders must co-operate to combat increasingly complex frauds. Outside the tight-knit EU community, it would be vital for the UK to ensure cross-border collaboration and international co-operation in the fight against rising fraud. It is, however, in all parties' interests to work together.

£190BN annual cost of fraud in the UK

£100BN estimated value of money laundered through the UK each year

3.4M annual number of incidents of fraud in England and Wales alone

National Crime Agency 2018

MILLENNIALS

Digital natives are tempting targets for fraudsters

Growing up with digital tech has meant the millennial generation is more comfortable with sharing their data, but it has left them likely victims of financial fraud

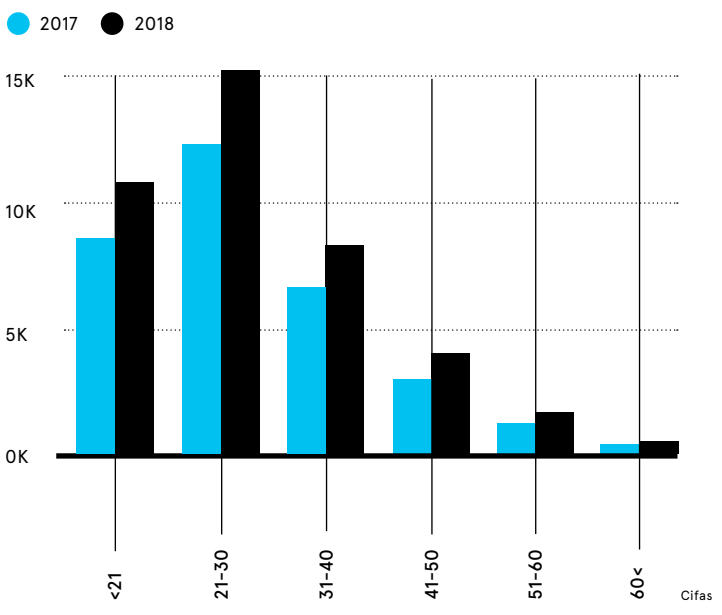
Josie Cox

In January, when Niraj Virji and his girlfriend were preparing to buy their first home, the 27 year old noticed something was wrong. Despite always paying his bills on time, he was told his credit rating was terrible.

"It was strange and I must admit I was quite shocked," says Mr Virji, who works as a buyer for WHSmith. Over the following weeks, he gradually understood he'd become the victim of an elaborate and complex case of identity theft and financial fraud, the repercussions of which would impact him for months.

Though Mr Virji is still unsure how fraudsters managed to swipe his personal information, allowing them to change his home address with the Driver and Vehicle Licensing Agency as well as on the electoral register. They then took out two loans in his name, with a combined value of almost £20,000. They opened several bank accounts and maxed out a credit card. They even tried buying a BMW. Mr Virji was oblivious to all this because any related correspondence was going to an address that wasn't his.

RISE IN THE NUMBER OF MONEY MULE ACCOUNTS BY AGE GROUP



"When I understood the true extent of the damage, it was just awful," he says. "The worst thing was that when I tried to explain myself, some of the banks and financial institutions just didn't believe me. I felt like there was a black mark against my name for ages. I even had debt collectors calling me."

Mr Virji's experience is an extreme example of the potential risks associated with impersonation scams, but less severe incidents of personal information theft are occurring daily. In an on-demand economy, where cash is swiftly becoming a relic of the past and e-payments the norm, it's increasingly common for spenders, particularly millennials, to lose sight of where their money is going and, crucially, whether it's reaching the intended recipient.

"Millennials are digital natives who freely use digital channels and are happier [than other demographics] to share data," explains Richard Petley, UK head of tech giant Oracle. "Their use of apps is integrated into their everyday lives and they expect financial services to be a seamless part of this digital lifestyle. In some cases, they may have more of a propensity to try out new services on digital platforms, which can create a higher susceptibility to financial fraud unless proper checks have been conducted."

According to research recently published by Lloyds Banking Group, there was a near four-fold increase in the number of 18 to 34 year olds being caught out by impersonation scams in the year to July, making that demographic, along with the over 55 year olds, the most at risk of being the target of financial fraud.

Millennials are more likely than their older peers to have grown up with mobile phones and the internet, which means they tend to be more trusting of virtual services in entertainment, retail and transport, but also banking. And anecdotal evidence suggests they're less likely to check their bank statements regularly if they don't get alerts on their smartphone.

"An increase in people living on their mobile phones and the expectation that all the things you can do on them are safe, for example using social media, being able to spend money at the touch of a button and having access to any information you want at any time, has unfortunately led to a rise in scams and fraud, as well as other serious crimes," says Natasha Vernier, head of financial crime at Monzo bank.

"It is really important our younger customers are educated on the risks involved in making payments to people posing as investors on social media and more generally on the risks that come with trusting everything found online or on mobile phones."

Impersonation scams usually involve somebody pretending to

> **Apps are integrated into their everyday lives and they expect financial services to be a seamless part of this digital lifestyle**

Ascannio/Shutterstock

Monzo

Though there is evidence that digital banking has made customers more susceptible to financial fraud, Monzo says its technology has actually made it easier to spot anything unusual and take swift action against any form of risk.

The more than three million customers of the challenger bank get instant notifications the moment they pay for something, enabling them to spot an unauthorised use of their card immediately. They can then freeze their card instantly in the Monzo app.

Natasha Vernier, Monzo's head of financial crime, says that because of this technology her team has been able to spot signs of a data breach at other companies before these have even been made public.

For example, the company alerted Ticketmaster in April last year when it detected high levels of suspicious activity in bank accounts used to make payments to the ticketing business. Ticketmaster later confirmed that a breach had occurred, affecting thousands of its customers.

"When British Airways was affected by a similar data breach, we identified the 1,300 Monzo customers who had been affected and ordered them replacement cards as a precaution," says Ms Vernier.

Monzo has also built a proprietary 3D Secure system which verifies online purchases in-app.

"More generally, Monzo does not rely on passwords to access the app, but just on the customer's PIN to make payments, because passwords are inherently insecure. Who hasn't used the same password twice?," says Ms Vernier. "And we never contact our customers by SMS as this is easy to spoof and a route for a large amount of social engineering scams."

be from law enforcement or a bank and asking the victim to transfer money into a supposedly safe bank account. But financial fraud is taking on many increasingly sophisticated guises. The challenge to stay safe is becoming like a burdensome game of tag.

An extensive report on the matter published by KPMG earlier this year found that banks across all regions of the world consider cybercrimes, notably hacks and data breaches, to be the greatest challenge in the field of fraud risk. The report also highlights that the pace of technological developments means constant innovation is critical to safeguard defences.

"In the context of a changing global banking landscape, where the demand for face-to-face banking is decreasing, volumes of digital payments are increasing and payments are being processed in seconds, fraudsters are creatively finding new ways to steal from banks and their customers," according to Natalie Faulkner, KPMG's global fraud lead. "Banks need to be agile to respond to new threats, and embrace new approaches and technologies to predict and prevent fraud."

Appetite for new technologies to help combat this rise in cybercrime is something a whole spectrum of organisations, from large, established businesses to fledgling startups, is capitalising on. Several companies are exploring the use of biometrics and tokenisation to safeguard customers' sensitive personal information, particularly among millennials.

In tokenisation, each transaction is completed by generating a unique token which allows a customer's sensitive data to be stored remotely. NatWest, meanwhile, in early October announced it was launching a three-month trial of biometric fingerprint credit cards in partnership with Mastercard and the software company Gemalto. The bank says the credit cards would offer contactless payments using fingerprint verification for transactions up to £100. Previously, NatWest had launched a trial for transactions up to £30.

"This is the biggest development in card technology in recent years and not having to enter a PIN not only increases security, but also makes it easier for our customers when paying for goods or services," says Georgina Bulkeley, director of strategy and innovation at NatWest.

Bob Reany, executive vice president for identity solutions at Mastercard, echoes this. "Feeling confident that your information is protected is paramount," he says. "Biometrics are more secure, more trusted and better suited to a world that requires more frequent authentication."

Intelligence is vital when dealing with 'friendly' fraud

With "friendly" fraud growing rapidly, merchants should see chargebacks as an opportunity to improve the consumer experience

The payments ecosystem has been transformed with new technologies offering more choice to consumers who now demand faster, frictionless transactions. Most investment has focused on the front-end of payments to increase the speed and frequency of transactions.

In comparison, historically there has been little to no investment in supporting the 2 per cent of transactions that result in chargebacks, since the original chargeback platform was developed in the mid-1970s. This is despite predictions from Chargebacks911 that so-called friendly fraud, whereby consumers seek to abuse the chargeback system to get a refund, will cost merchants upwards of $250 billion a year by 2020.

This lack of investment spiked a change in 2018 when Visa launched its Visa Claims Resolution programme. Now the conversation is changing and the industry is realising it can no longer write off the cost of chargebacks for fear of upsetting their customers, whether on the merchant or issuer's side.

Even with these new systems being put into place, chargeback growth in the UK is outpacing the growth of online transactions threefold, fuelled by the fact that two out of five consumers who commit friendly fraud do it again within 60 days.

"The problem costs both issuers and merchants," says Monica Eaton-Cardone, chief operating officer at Chargebacks911, a chargeback management solution that helps online businesses and institutions minimise loss, mitigate risk, recover lost revenue and enhance the customer experience.

"We've seen a 20 per cent growth in chargebacks year on year, with friendly fraud doubling. Yet only 18 per cent of claims are estimated to be disputed, since most merchants and acquirers don't have the technology or resources to manage the costly disputes.

"The dispute process is still quite archaic. It takes a lot of time, it's not codified, there's a lack of intelligence and there are no standardised procedures in place. Three quarters of banks we surveyed in Europe said their entire processing department for chargebacks and disputes was manual.

"There is no way you can scale this without some kind of intelligence and consistency. Consequently, consumers are exploiting that gap. This is the Achilles' heel in the mission of protecting consumers, scaling at the rate required to match the surge of online growth."

While it's crucial that merchants and acquirers are able to challenge chargebacks in a cost-efficient and streamlined way, it's important they see these claims as an opportunity to improve the consumer experience, rather seeing customers as the enemy.

In a world of emerging payment methods, chargebacks are a huge differentiator for card associations. No other payment method offers such a mechanism for assurance.

Chargebacks911's tools work exclusively in the post-transaction environment, helping to increase the speed at which disputes and chargebacks can be shown to be valid or invalid.

The company's platform leverages artificial intelligence and machine-learning to identify the source of the chargeback before submitting the evidence to the acquirer, card scheme or issuer. This intelligence helps merchants retrieve lost earnings from friendly fraud, ensure consumers are given a fair solution and provides issuers with valuable feedback that improves future decision-making in this area. It's a win-win-win.

"We also provide feedback to the fraud filter so you don't run the risk of blacklisting every customer who files a chargeback," says Ms Eaton-Cardone. "Not all chargebacks are equal.

"Because we're enabling fair and balanced decisions for everyone, we're also able to help repair the relationship between merchants and their customers who'll, hopefully, not only stop attempting friendly fraud, but also continue to do business with that company.

"Everything we do is data driven and we have invested a terrific amount in automating virtually every cycle of a payment dispute to improve quality and consistency across the board. We help foster a more digital environment so, instead of waiting for legacy systems that require a lot of manual work and lag 30 to 60 days before disputes are resolved, you can use intelligence right after that transaction settles.

"We will continue to help revolutionise and streamline the process, investing in intelligence that helps all counterparts in their unified mission to protect the consumer experience."

$250bn

Chargebacks911 predicts friendly fraud will cost merchants upwards of $250 billion per year by 2020

2 out of 5

consumers who commit friendly fraud do it again within 60 days

only 18%

of chargebacks are estimated to be disputed, since many merchants and acquirers don't have the technology or resources to manage the costly disputes

For more information please visit chargebacks911.com

CHARGEBACKS911 CHALLENGE THE STATUS QUO

Companies seek visibility in fight against insider threats

With insider fraud threats continuing to grow in the digital age, organisations require a clear and accurate understanding of what users are doing and how they are interacting with data

Rapid advancements in technology in recent years have given businesses far greater mobility, accessibility and interconnectivity. Though this has provided enormous value, it has also meant more users have the capability to commit harmful behaviour, fraudulent or otherwise. The growing popularity of remote working has compounded this risk further by enabling users to commit malicious activity from wherever they are in the world.

Organisations are no longer just bricks and mortar. Contracting and outsourcing are also on the rise as companies are trying to keep pace in a more competitive space, leading to less human oversight and an environment where insider fraud can become more prevalent and difficult to detect. Assets come and go every day, meaning they can no longer rely on perimeter security. They need complete visibility both on and off the corporate network.

The *2019 Insider Threat Intelligence Report*, which collects data from Dtex Systems' risk assessment findings over the previous year, found some form of undetected insider threat in every assessment, including high-risk data transfers via USB or cloud and employees using personal webmail. Users were found to be bypassing security in 95 per cent of assessments and in 98 per cent of assessments Dtex found proprietary company data that was publicly accessible on the web.

According to the *2018 Cost of Insider Threats Report*, insider threats cost businesses an average of $8 million an incident. Yet until a few years ago, users accessing data within an organisation almost entirely evaded the attention of security teams. Today insider fraud is increasingly prevalent and companies struggle to even detect it in the first place.

"All businesses, no matter the industry, are at risk of malicious insiders," says Armaan Mahbod, manager of insider threat and cybersecurity investigation at Dtex Systems. "These malicious actors can come from any role, not just pre-determined groups of 'high-risk' job titles. Therefore, a continuous audit trail of all users, devices and applications within an organisation is critical to catch warning signs and conduct effective investigations.

"Organisations are often too late and tracks have already been covered. In a recent phishing attack on an Australian university, for example, they didn't have the audit trail to effectively investigate after the incident, which severely hampered their recovery and response."

Companies typically have some form of fraud controls in place, including thresholds and limits, to identify specific transactions. However, many offenders are high-level executives, managers or otherwise, who are fully aware of the limits and go below the thresholds to avoid detection from suspect transactions. They may steal smaller quantities of data or money over a long period, resulting in the largest cumulative value stolen.

Most commonly, the individuals that are committing malicious insider activity are people in positions of trust, who already have some level of authorised access to critical systems. This is why it is so important to understand the insider threat kill chain, says Mr Mahbod.

"Methods for intrusion and exfiltration are constantly evolving, but it is nearly universal that malicious insiders will attempt to cover their tracks, or circumvent security tools or alerting thresholds," he adds. "We consistently find that investment in detecting these early stages of the kill chain, like covering tracks or security bypass, gives organisations the best return and results. Just as one example, Dtex caught data theft by a foreign national at one of our customers, AMP, due to the culprit's attempts to circumvent company security."

There are two factors that make insiders a greater fraud threat than outside attackers. Their malicious attacks are not premeditated and they rarely act immediately after being brought into an organisation. Instead, they slowly accumulate insights on all the traps set in place. Secondly, inside attackers generally have some level of authorised access, either in their current role or a previous role within the same company.

> **Organisations cannot defend against attacks that they cannot see... With greater visibility comes greater certainty, which translates to more efficient investigations**

Malicious insiders, who are responsible for 22 per cent of all insider threats, primarily use permitted applications to evade detection, including uploading data to online file-sharing sites sanctioned for business use, utilising personal webmail accounts that aren't monitored and unblocked data-dumping websites.

In Dtex's report, 95 per cent of assessments also identified employees using anonymous and private browsing, which was an increase from 60 per cent the year before. When there is no malicious intent, threats can be even more difficult to detect, as is the case with the 68 per cent of insider threats that are purely down to negligent users causing accidental harm. This makes the visibility of user behaviour across the entire organisation crucial.

"Organisations cannot defend against attacks that they cannot see," says Mr Mahbod. "Also, placing monitors on critical systems is not enough because it only gives you less than half the full story. When a malicious insider steals data from a critical system, transferring the data to their own device, what did they do next? With greater visibility comes greater certainty, which translates to more efficient investigations.

"On the flip side, when you don't have visibility across an organisation and look at a specific device or IP address for security incidents, you run the risk of creating too many false positives because your solution does not have all the organisational domain context it needs to determine whether an activity is high risk. You need historical activity of the user, a comparison to their peers and the organisation to make a stronger determination."

Dtex Systems provides the comprehensive end-point visibility that companies need at scale to understand, in near real time, any abnormal user behaviours which have led to identification of fraudulent behaviour. Furthermore, Dtex's data highlights the contextual information necessary to understand the bigger picture behind users' malicious actions.

"Through this visibility and the elevation of anomalous behaviour, Dtex enables organisations to be 'left of boom', which means the organisation is building and running a security posture that gets out in front of the threat, allowing security teams to act before an incident, not just respond after the fact," says Mr Mahbod. "By seeing the full kill chain of events, companies are able to identify suspicious behaviour prior to events actually harming the business. This allows organisations to be proactive rather than reactive."

For more information please visit dtexsystems.com

100%
of assessments found instances of high-risk data transfer via USB or cloud applications and employees accessing and using personal email accounts on corporate endpoints

98%
found customer proprietary information publicly accessible on the web

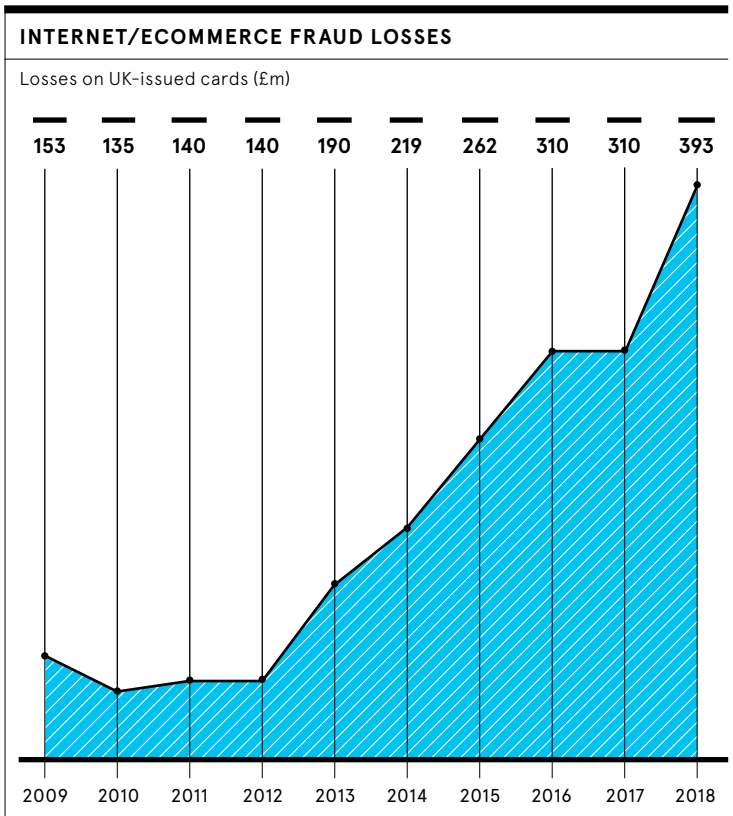
97%
found instances of employees engaging in flight risk behaviour

95%
found users actively attempting to circumvent corporate security policies

74%
saw the use of unsanctioned portable applications, which are increasingly being used to bypass security

Dtex systems 2019 insider threat intelligence report


Andrew Neel/Unsplash



ECOMMERCE

Identifying and tackling online fraud with AI

Artificial intelligence (AI) can help retailers rapidly identify and prevent ecommerce fraud, but human oversight is still essential

Duncan Jeffries

Thanks to the internet, we no longer need to go to the shops; instead, the shops come to us. In a few clicks you can order everything from the latest digital gadgets to dog food, from the comfort of your sofa. And same-day delivery options mean you can receive items faster than ever.

But the speedy online transactions and one-click purchasing systems that underpin the ecommerce sector don't just make life easier for consumers; they make things easier for fraudsters too.

Successful ecommerce retailers receive thousands of orders a day, and these card-not-present (CNP) purchases are harder to verify than those where the card and cardholder are physically present. In fact, a study by LexisNexis Risk Solutions found that fraud via remote channels, such as online and mobile, is up to seven times harder to prevent than fraud in person.

So if an online retailer's ecommerce fraud prevention system isn't up to scratch, it can cost them dearly. Indeed, Juniper Research predicts that CNP fraud could cost online retailers more than £58 billion over the next few years.

The tools and techniques criminals use to carry out chargeback fraud, where the consumer makes an online purchase with their own credit card and requests a chargeback from their bank after receiving the item, or take over online accounts are constantly changing and increasingly sophisticated.

"Traditional approaches to fighting fraud, such as rules engines and scoring, are too fixed to adapt to this shape-shifting nature of fraud," says Eido Gal, co-founder and chief executive of Riskified, which provides an ecommerce fraud prevention solution and chargeback protection service for high-volume and enterprise merchants.

Mr Gal claims AI solutions that learn from each transaction and improve their accuracy are much more effective than these legacy methods of ecommerce fraud prevention.

"Fraudsters take many different approaches to appear as a legitimate cardholder," he says. "They may use a proxy, spoof a device or take over a cardholder's retail account. A well-designed AI solution examines the links across these datapoints, compares them with historic orders and instantly determines when something is wrong."

AI and machine-learning tools look at hundreds of datapoints across billions of transactions to identify patterns that might constitute fraud.

> **[With AI] retailers have the sort of broad vision necessary to spot fraud and orders that are far out of the norm**

What's more, they can find cases of fraud that no human is likely to spot.

"By deploying constantly learning machines that use the data from many thousands of merchants around the world, retailers have the sort of broad vision necessary to spot fraud and orders that are far out of the norm," says Ed Whitehead, managing director, Europe, Middle East and Africa, at Signifyd, a fraud protection company that detects fraud and reimburses merchants for fraudulent chargebacks on approved orders.

When AI recognises an outlier order, it can either automatically block it or refer it to a human expert for review. "The best way to use AI is to use it to solve the simple cases," says Paul Weathersby, senior director of product management at LexisNexis Risk Solutions UK.

"A person is better at making decisions, so you could use the machine for cases which are fairly easy to process and improve the customer experience, and then pull out the exceptions that someone needs to look at."

Mr Whitehead agrees that a degree of human oversight is a key part of effective AI-based ecommerce fraud prevention. "There are certain tasks that machines are good at, those requiring speed and scale, and there are tasks that humans are good at, those requiring intuition and experience," he says. "Combining the two creates a powerful shield to fraud while also recognising legitimate orders that might include some red flags."

Data feeding into an unsupervised machine-learning model also needs to be properly monitored. Otherwise, says Mr Weathersby: "The vast amounts of data an unsupervised model works through can produce rules that don't make sense based on data which is quite hard to locate."

He adds that if the method for supplying a machine-learning tool with feedback on what constitutes a good or bad decision is inconsistent, "then the machine will start to learn things which a human would quite clearly understand are not correct".

This could, for example, result in AI that becomes more conservative as time goes on. "For instance, each time a fraudulent order is shipped and comes back as a chargeback, the machine learns not to ship similar orders," says Mr Whitehead. "Eventually, the machine ratchets down the number of orders a merchant is shipping and invariably some of the declined orders were actually legitimate."

Criminals will always look to circumvent the ecommerce fraud prevention systems that merchants put in place and some are already using AI for just this purpose. It's therefore essential that online retailers employ multiple methods of ecommerce fraud prevention and layers of control, says Jackie Barwell, director of fraud product management at ACI Worldwide.

Positive profiling, for instance, builds a comprehensive picture of customers at the individual level through behavioural data, externally confirmed fraud intelligence and a wide range of customer identifiers. "Rather than the traditional route of screening each transaction, this focuses fraud screening on the person behind that transaction," Ms Barwell explains.

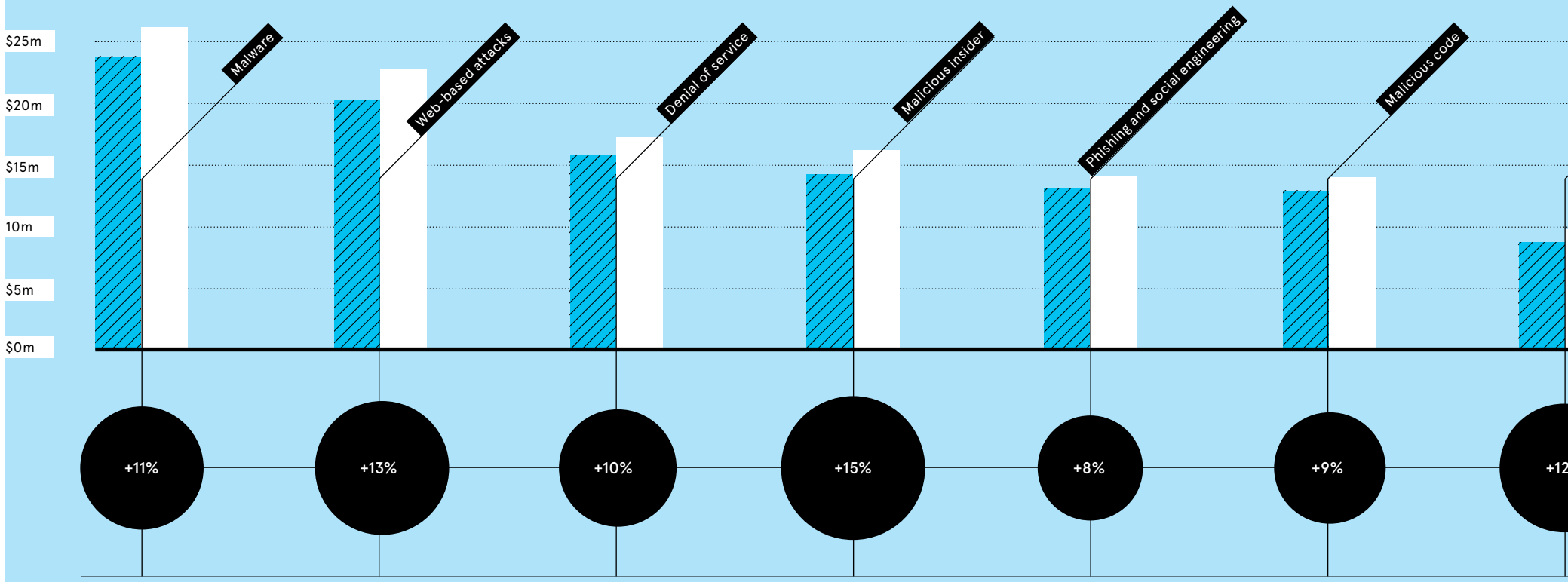
She adds that the technique is especially useful for new ecommerce methods such as click and collect, "where there is not as much time available to conduct post-transaction, real-time analysis".

Other new ecommerce services will no doubt arrive in the future and fraudsters will inevitably seek to exploit them. But as long as online retailers have AI in their armoury, they should manage to stay ahead of cybercriminals looking to profit from one of modern life's greatest gifts, the option to shop from the comfort of your home.

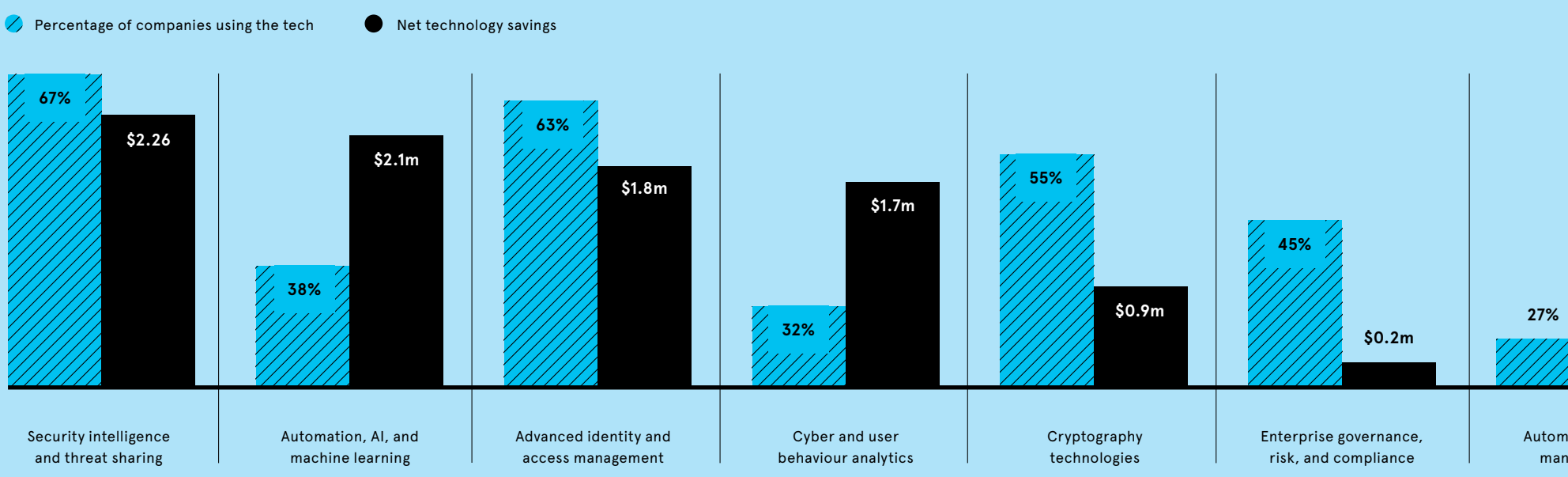
THE REAL COST OF CYBERCRIME

Cybercrime can impact an organisation's reputation, customer base and ability to function, but the cost of poor cybersecurity is never clearer than when looking at the money companies stand to lose

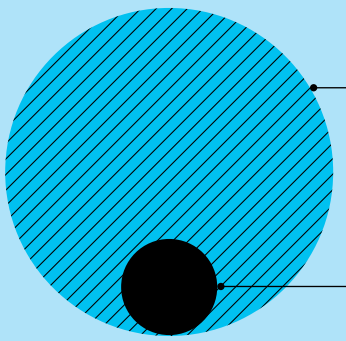
AVERAGE ANNUAL COST OF CYBERCRIME BY TYPE OF ATTACK



HOW MUCH CYBERSECURITY TECHNOLOGY CAN SAVE COMPANIES



GLOBAL VALUE AT RISK FROM DIRECT AND INDIRECT CYBERATTACKS, CUMULATIVE 2019 TO 2023



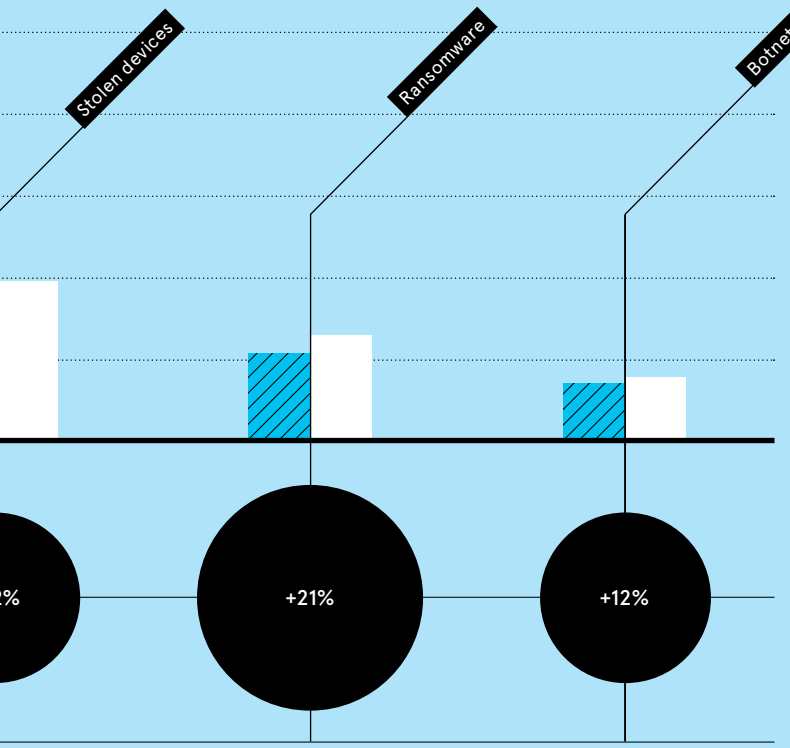
77%

Value at risk from direct attacks

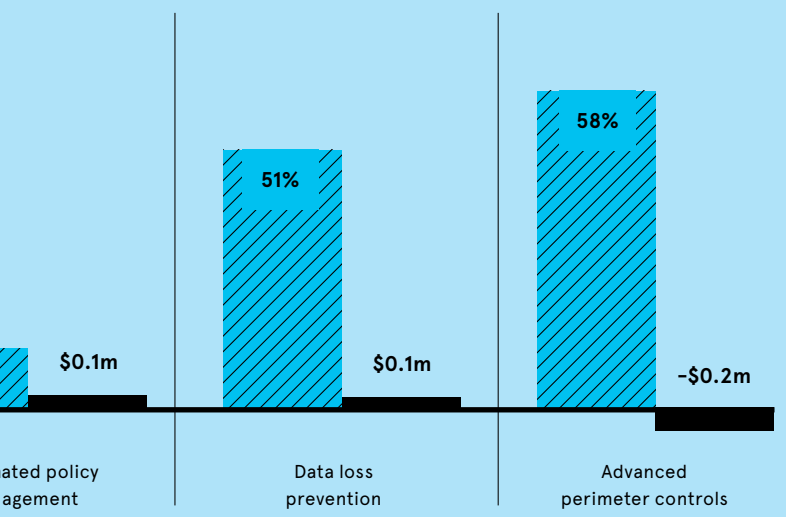
23%

Value at risk from indirect attacks

Accenture 2019



Accenture 2019



Accenture 2019

CYBERCRIME COSTS AROUND THE WORLD

Average annual cost of cyber attacks (in million US dollars)

$27.4m
USA

$13.6m
JAPAN

$13.1m
GERMANY

$11.5m
UK

$9.7m
FRANCE

$9.3m
SINGAPORE

$9.3m
CANADA

$8.1m
SPAIN

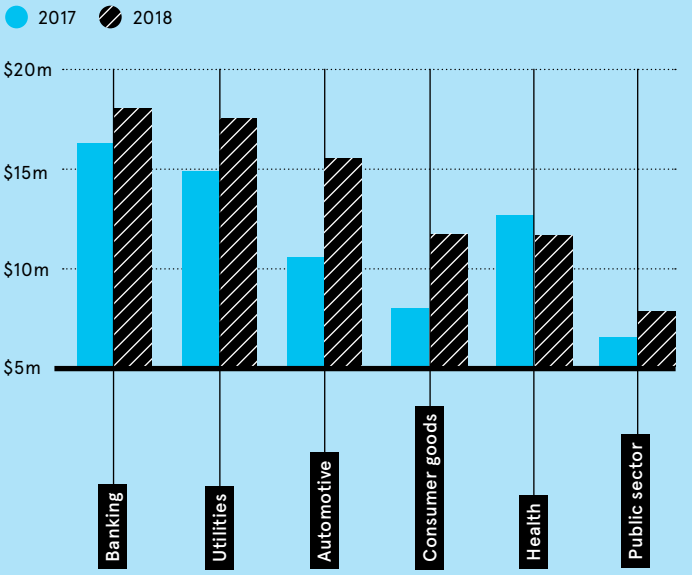
$8m
ITALY

$7.2m
BRAZIL

$6.8m
AUSTRALIA

Ponemon Institute/Accenture 2018

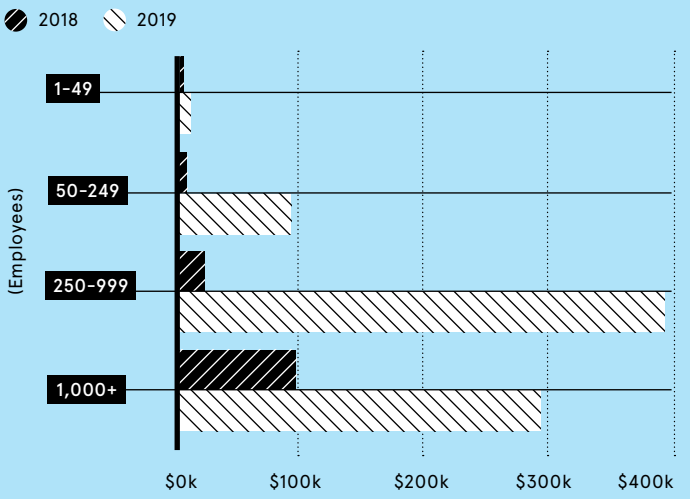
AVERAGE ANNUAL COST OF CYBERCRIME BY INDUSTRY



Accenture 2019

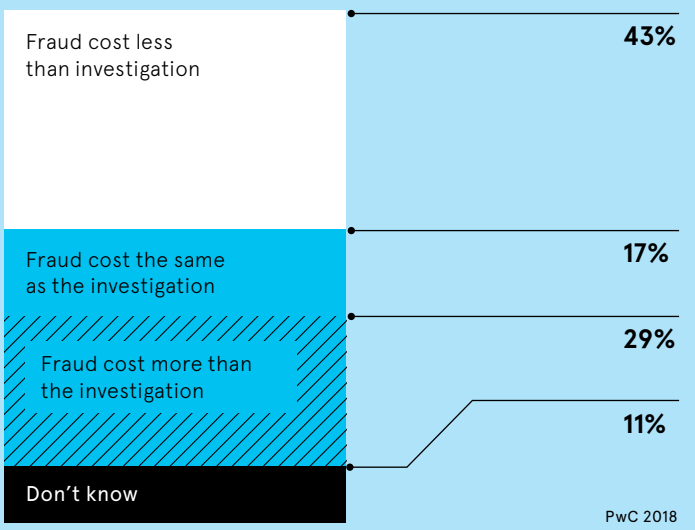
COST OF LARGEST SINGLE CYBERATTACK TO EUROPEAN AND US FIRMS

Average cost by company size



Hiscox 2019

TIME SPENT INVESTIGATING FRAUD CAN COST MORE THAN THE FRAUD ITSELF



PwC 2018

PHISHING

Five phishing scams your business needs to know about

Verizon's *2019 Data Breach Investigations Report* found C-level executives are 12 times more likely to be targeted by phishing scams than in previous years, with phishing involved in 33 per cent of data breaches last year. Here are five common phishing scams to guard against

Davey Winder

HR or finance department salary switcheroo fraud

This is one of those phishing scams that you might think would never work, yet the evidence suggests it does. Call it “customer-authorised fraud” or simply “impersonation”, but getting a salary diverted into a fraudulent account is easier than it sounds.

“Generally they will make out that something has changed, trying to trigger a click and submission of bank details into a phishing version of a real payroll site that the hacker believes the company is using," says Matt Aldridge, senior solutions architect at Webroot.

With good intelligence about the payroll system in use, the social engineer, or crook, can craft a believable email and clone a site with legitimate logos and a closely matching url.

"In this way they can capture the real login details and divert the funds at a time of their choosing," Mr Aldridge warns. "These types of attacks can be very lucrative if well executed against a poorly trained and poorly protected human resources team.”

This is because fraudsters "recognise the value of attacking using multiple weakness points”, according to Omri Kletter, head of fraud, Europe, Middle East and Africa, at NICE Actimize.

The challenge of detecting such attacks can be more difficult than in a retail environment, say, because the normal behaviour of a business is "often unpredictable and complex, and the beneficiaries multiple and international”, Mr Kletter points out.

Make sure the HR department know the fraud exists and "put in place a process which carries out a check through an independent route to the individual concerned”, says Dr Guy Bunker, chief technology officer of Clearswift.

Supply chain trust ‘ladder-climbing' fraud

How well do you know your suppliers? You probably don't know their processes as well as the level of trust you invest in your dealings with them would suggest.

"Supply chain trust works both ways," says Jake Moore, cybersecurity specialist at ESET. “You are as strong as your weakest link, but when this link is offsite and embedded in another company, you won’t know a vulnerability exists in the first place." It is this that cybercriminals exploit in the supply chain trust ladder-climbing fraud exploit.

"They work their way up the supply chain to bigger, better targets, using compromised email accounts of suppliers to exploit existing relationships,” explains Cath Goulding, Nominet's chief information security officer.

The clever part of these phishing attacks is they are really hard to spot as they originate from an already trusted source. "This can trick finance teams into paying false invoices or sharing shipping information with the wrong parties, which in the current General Data Protection Regulation world could lead to large fines for the business,” Ms Goulding warns.

Think you'd never fall for a phishing scam that spoofs invoices from third parties with whom established relationships and payment history already exist? Think again. "Both Facebook and Google were duped in this way between 2013 and 2015, ultimately to tune of $100 million,” says David Mount, European director at Cofense.

However, tightening up financial controls makes it much harder for attacks against employees to succeed.

Bypassing two-factor authentication

Two-factor authentication (2FA) is kryptonite to cybercriminals, preventing many an otherwise dead-cert data breach by adding an additional layer of security into the user-credentials mix.

"As 2FA is becoming more prevalent in enterprises, simple brute-forcing, or sniffing, of passwords is not enough,” says Javvad Malik, security awareness advocate at KnowBe4.

Phishing scams, often looking to steal sensitive data and penetrate networks for the long term, are sophisticated and involve "multiple stages to take users to loading pages, which bypass any webpage filtering, and from there to the desired malicious page”, says Mr Malik.

The bad news is that it is becoming easier and easier for the cybercriminals to do this. "Recently on the dark market, we have seen new phishing kits that allow for the intercepting or mirroring of 2FA requests," says James Houghton, chief executive at PhishingTackle. "The visitor to the website assumes this is safe when, in fact, there is a 'man in the middle' exploiting that layer of security."

Think of these as the equivalent of a cashpoint-card skimming façade being attached to the front of a legitimate machine to capture your PIN.

The fact that 2FA is increasingly understood to be “more secure” than a password alone, ironically makes this phishing scam easier to pull off as users are lulled into a false sense of security.

"User awareness is one of the only defences against this," Mr Malik advises, "and so they should be on the lookout for text messages or emails claiming to be from a service provider with a link to enter 2FA credentials."

Deepfake audio-phishing

If you thought deepfakes were just fake news videos designed to spread misinformation at election time, you would be wrong. Deepfake audio, the computer-generated synthesis of a real voice that can be manipulated to say anything, has arrived on the phishing scams radar.

According to Dr Matthew Aylett, chief scientific officer at CereProc, this weaponisation of deepfake audio "has already cost businesses millions through sinister new telephone fraud and scams".

Oh yes, remember that not all phishing is carried out by email; telephone phishing is a very real threat.

"By using deepfake audio to replicate a boss, manager or colleague's voice," says Dr Aylett, "HR teams could be duped into sharing confidential personal information and finance teams into handing over bank account details or transferring money to a third party."

His concerns follow a Symantec warning that three chief executives were tricked by deepfake audio into transferring millions of dollars. "Hackers replicate the voices of business pros in a position of power using AI-enabled speech synthesis technology and at present there is no defence against telephone-phishing scams such as these," Dr Aylett warns.

"Employees must understand the red flags that might reveal they're being targeted by deepfake audio," he advises. "They should ask themselves, 'Does this person's voice sound completely natural?' If in doubt, hang up."

Phishing in the cloud

Brand impersonation spear-phishing attacks featuring cloud providers such as AWS and Microsoft Azure are becoming increasingly common.

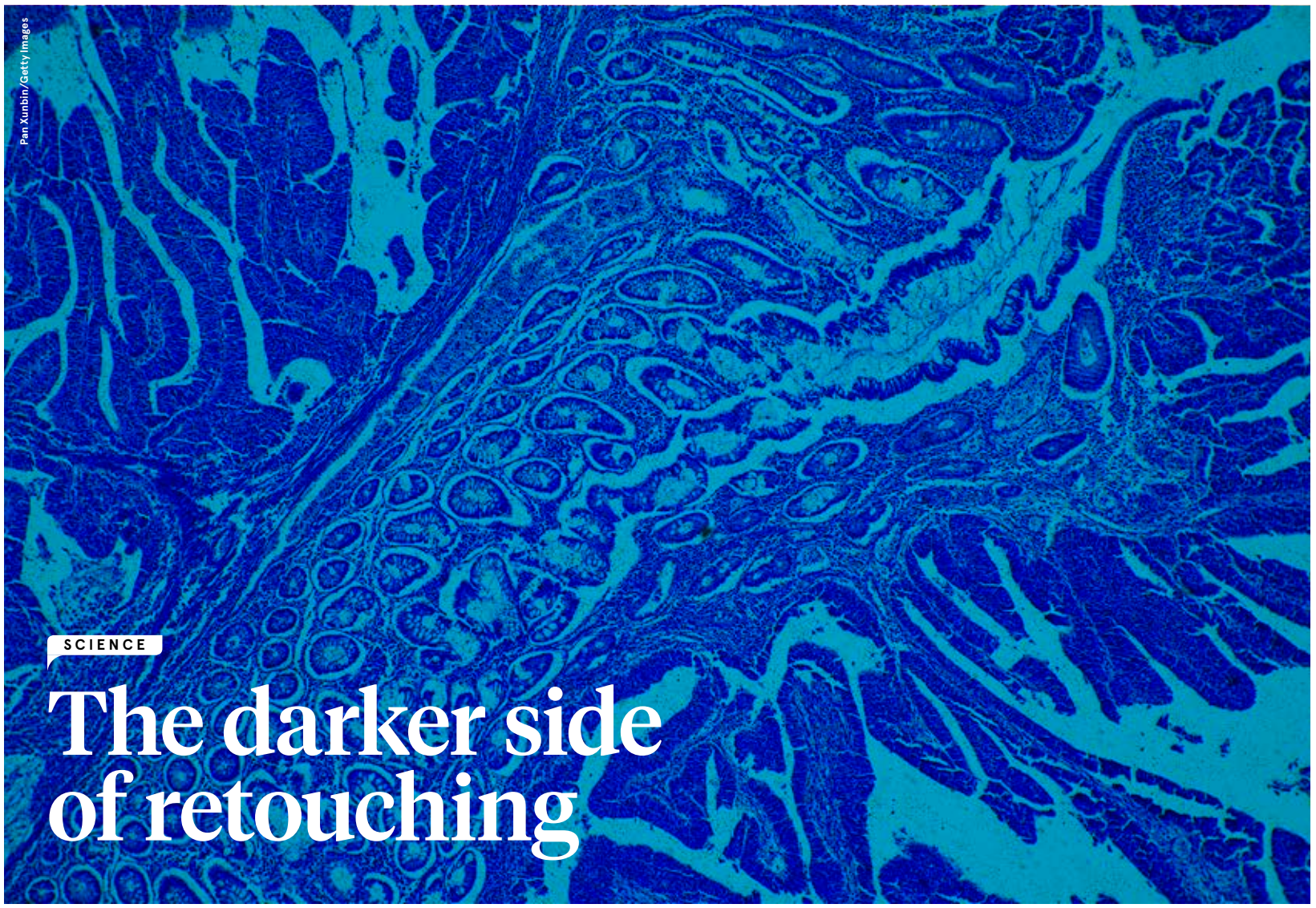
Steven Peake, pre-sales engineer at Barracuda Networks, says recent research by the company found 83 per cent of spear-phishing attacks involved brand impersonation and 40 per cent impersonated cloud providers. Analysis from FireEye also revealed attackers are getting ahead by using the cloud in phishing scams.

"Our most recent analysis showed how attackers are adapting their tactics, techniques and targets to changes in security defences," Jens Monrad, head of intelligence, Europe, Middle East and Africa, at FireEye, explains.

The research also found those most at risk were Microsoft users. "Sixty-eight per cent of phishing attacks use Microsoft branding and are also using cloud services more frequently to target businesses," says Mr Monrad. Microsoft and Office 365 phishing attacks increased by 12 per cent quarter over quarter.

The most common cloud-phishing scam techniques included spoofed emails, evasions based on captcha (completely automated public Turing test to tell computers and humans apart), multiple urls to mask a malicious link and nested-phishing techniques, which use message attachments containing phishing urls.

"Knowing and learning from past incidents, as well as having insights into the ever-changing cyberthreat landscape, can help organisations better prepare, prioritise and remediate the threat," Mr Monrad concludes.



Pan Xunbin/Getty Images

SCIENCE

The darker side of retouching

Adenocarcinoma of human tumor tissue micrograph

Image manipulation has been a part of modern life for years, but when medical images are being manipulated, lives and livelihoods could be at stake

Gemma Milne

Image-editing technology enables manipulation of all kinds. There are apps to brighten skin and remove blemishes or, more worryingly, tech to make deepfake videos, convincingly substituting Jack Nicholson for Jim Carrey in a doctored film clip. For some industries, this technology can be a welcome innovation, but not for the health sector, where science and medical fraud is on the rise.

So what is the best option for fraud prevention? Currently, it's our pattern-finding, anomaly-spotting human brain, and lots of time. And, unfortunately for those impacted by science and medical fraud, artificial intelligence is not yet able to replace our human knack.

Misconduct in science and academia can take many forms, including plagiarism, edited data and omission of conflicting reporting. And academic credibility is largely based on a publishing record: which journals, how often, and the number of citations. But the so-called pressure of "publish or perish" may lead the unscrupulous to falsify data, resulting in fraudulent research.

Automated systems for spotting simpler forms of fake research have improved in recent years, but possible loopholes remain. Editing slides captured from microscopes by copying and pasting flipped, mirrored or rotated cropped images is a concerning development. These images can then be embedded in scientific papers to prop up unproven claims.

Elisabeth Bik, independent science consultant and former microbiology researcher at Stanford University, is a self-appointed sleuth of misconduct in science. She monitors published biomedical papers looking for suspected manipulated images, reviews them in the PubPeer blog and, when she is sure there is evidence of foul play, reports her findings to the journals concerned.

"I'm really frustrated; with all the cases I've submitted, few of them have actually been addressed," says Dr Bik. In 2016, she published research detailing 20,000 papers she investigated, 4 per cent of which she claims contained doctored images. Some of these 800 papers are still being investigated three years later.

Dr Bik accuses journal editors of being notoriously slow or resistant to investigate allegations of misconduct in science because of the time and effort required to correct or retract the research. She also posts her findings on Twitter, to drum up public outrage and prompt journals to act. "I feel once the evidence is out there, they have to investigate," she insists.

There is currently no effective automated system to spot manipulations, so journals cannot weed out fraudulent submissions at the start of the publication process.

Ivan Oransky, co-founder of the science misconduct media outlet Retraction Watch, which tracks papers removed from scientific journals, says: "It's like looking at murder conviction rates as a proxy for the number of murders; we know there are far more murders than convictions."

Medical fraud is an area of serious concern. Having staff manually searching for irregularities in images submitted for approval to insurance companies is too costly and, without an automated system for flagging questionable

> **"I'm really frustrated; with all the cases I've submitted, few of them have actually been addressed**

"evidence", fraud prevention is almost impossible.

Numerous kinds of medical fraud rely on images, for instance pictures of injuries to show effects over time or photographs of accidents. Timestamps and dates can be easily edited in image metadata and switched GPS locations can also falsify claims.

Most medical fraud, however, may happen at the provider level. Resubmitting anonymous x-rays across multiple patient claims, knowing the images won't be cross-referenced, is a common allegation.

Researchers at the University of Portsmouth estimate medical fraud to be about 6 per cent of global healthcare spending at around £420 billion.

Insurance industry veteran Dan Gumpright says technology used to reduce human processing time is part of the reason medical fraud is so prevalent. "They [fraudsters] believe it's a victimless crime, even more so when there's no person on the other end of the line," he says. "A lot of insurance companies now process claims through a chatbot, email or a website; it's a lot easier psychologically."

But Mr Gumpright points out that it's not a victimless crime. "If people are committing fraud against insurance companies, it raises everyone's premium," he says. "Insurance companies are not eating the loss."

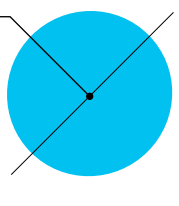
If fraudulent science is published in the biomedical field, ultimately patients can be harmed either from wasted time trying in vain to build upon false results or developing inappropriate therapies. If medical fraud in the insurance industry rises, so too do premiums and barriers to access for wider populations.

Though the incentives for misconduct in science and medical fraud differ – one for career progression, the other for financial gain – the 'loser' in both cases is the same. While we await tools to automate our human adeptness at spotting irregularities, the health and wealth of society remains at stake.

Insurance fraud in the UK is on the rise

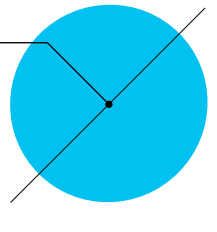
£11.9m

the combined value from 27 insurance fraud cases from 2014-2017



£17m

the combined value from 19 insurance fraud cases in 2018 alone



Fake insurance claims costing companies millions

Recent findings from KPMG's 2018 Fraud Barometer demonstrate a dramatic spike in insurance fraud. From faked car crashes to imaginary injury claims, insurance fraud in 2018 cost companies more than the preceding four years combined. One particularly drastic case saw a man jailed for nine years for masterminding a fraudulent insurance claim worth £4 million.

KPMG

Simultaneously evolving speed and security in payments

Economies are increasingly using real-time payments technology to meet the demands of a 24/7 tap-and-go lifestyle society

Value needs to shift faster and real-time payments offer tangible benefits, ensuring the instant availability of emergency funds after a natural disaster, for example, or immediately confirming payments to release urgent medical supplies.

As payments move faster security is paramount. Criminals may seek to exploit the convenience of faster payments for fraud or money laundering purposes. And when a payment settles instantly, the opportunity to recover funds is greatly reduced.

Speed and safety, therefore, must evolve in parallel to maintain integrity and security of the payments system.

While media attention has focused on consumer fraud in the context of real-time payments, banks are also collaborating to reduce the fraud risk across the global banking network.

Fighting back

"With real-time, cross-border payments, we need a new approach to fraud prevention that avoids and stops high-risk payments, rather than reporting after the fact," says Tony Wicks, head of financial crime compliance at payments co-operative SWIFT.

"The game has changed. Compliance teams need to make quick decisions, more so than ever before. It's increasingly important to try and take human error out of the equation. Transaction behaviour involves multiple institutions and is becoming more complex. So I think there will be increasing demand for tools and services at network level."

SWIFT is driving community-wide solutions to enable fast and secure payments. Its Customer Security Programme (CSP) is at the heart, prescribing a set of regularly updated mandatory controls to create consistent security practices across its entire community.

"All financial institutions must meet this set of standards using clearly defined controls," says Brett Lancaster, managing director and global head of customer security at SWIFT, who oversees the CSP. "All customers must attest their level of compliance every year. Failure to meet these controls means we report them to their local regulator."

Importantly, financial institutions can also access attestation data to assess counter party risk. The financial ecosystem is interlinked, so everybody cares about the weakest link in the chain.

"Our customers are taking this seriously," says Mr Lancaster. "About 95 per cent have attested to their compliance to the CSP controls covering about 99.5 per cent of all traffic across SWIFT."

People, process and technology

The co-operative has developed technology-based solutions, such as the real-time application programming interface, built into the global payments innovation (SWIFT gpi). Banks sending and receiving data over the SWIFT network can pre-check the beneficiary account information with the ultimate receiving bank. This minimises the risk of misdirection to other accounts. More broadly, the use of artificial intelligence (AI) facilitates rapid scanning of very large datasets, helping to identify potential problems before they are processed.

SWIFT recently launched Payment Controls, a new tool to prevent and detect fraud, which helps banks monitor and protect their core payments, by flagging and responding to fast-moving, suspect transactions efficiently.

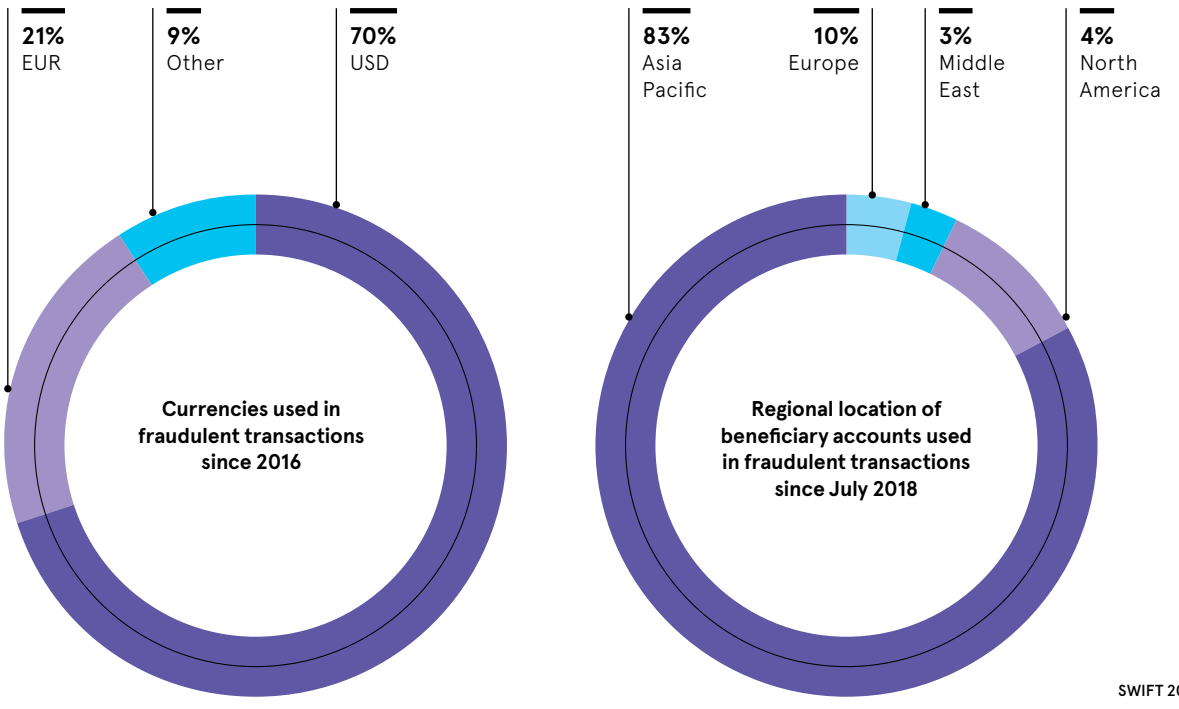
"The fact that you may have a payment refused because of fraud risk creates potential inconvenience for customers," says Mr Wicks. "So we need to make the systems and processes accurate and precise when detecting fraud. This means we can help minimise fraud risk, as well as the impact on legitimate transactions. We are using AI and other methods to improve outcomes for customers.

"In the world of compliance, people typically want to slow things down and take longer to make decisions. That's incompatible with the current thinking. So we need to change how we address these problems from a compliance perspective. If we can get this right, and I think we are going in the right direction, then it's the supporting fabric that will make a difference to instant payments, especially within the cross-border world."

> **With real-time, cross-border payments, we need a new approach to fraud prevention that avoids and stops high-risk payments, rather than reporting after the fact**

For more information please visit www.swift.com

FRAUDSTERS ARE SEEKING TO EXPLOIT THE CONVENIENCE OF REAL-TIME PAYMENTS



SWIFT 2019


Pressmaster/Shutterstock

CHIEF EXECUTIVE FRAUD

When insider threats come right from the top

Insider threats hitting the headlines tend to be perpetrated by middle or lower management, but when fraud is carried out by the C-suite, the costs can be eye-watering

Cath Everett

While fraud by a chief executive may not be common and is certainly the least talked about, it can be the most costly to an organisation.

According to the Association of Certified Fraud Examiners' *2018 Report to the Nations*, company owners and senior leaders may commit only 19 per cent of all frauds perpetrated, but such crime results in a median loss of $850,000 (£670,000) an incident.

This figure is nearly six times higher than the median loss brought about by middle managers and seventeen times more than that caused by low-level employees.

The study points out that high-level fraudsters generally have better access to an organisation's assets. They also have greater technical ability to commit and conceal fraud, and can use their authority to override controls or hide their crimes more easily than those further down the corporate ladder.

Such fraud can take a number of forms. In some cases, says Jose Hernandez, chief executive of organisational change consultancy Ortus Strategies and author of *Broken Business*, it is simply about senior executives circumventing company controls for their own personal gain. Invoice fraud, in which individuals submit invoices for suppliers that do not exist, is an example.

More commonly, leaders rationalise their unethical actions, such as tax avoidance or evasion, by convincing themselves they are necessary to deal with pressing business problems, says Mr Hernandez.

"It may involve individuals falsifying documents and financial records and presenting them to external auditors," he says. "Another form we encounter in global corruption investigations relates to using sham contracts with third parties to divert corporate money to improper beneficiaries, such as government officials."

But the implications for an organisation are significant at every level. Not only can subsequent investigations cost millions as they are often complex and take months or even years, but chief executive fraud also leads to major reputational damage, both internally and externally, not to mention the financial impact.

A key issue is this kind of behaviour undermines the trust and integrity of the entire company, which is why it is so rarely discussed. Indeed, misconduct at this level potentially has serious criminal and civil implications, not just for individuals, but also for the corporation, leading to falls in share price and a leadership vacuum.

As a result, says Ben Rose, chief underwriting officer at insurance company Digital Risks, the initial instinct of most businesses is to try to conceal the situation, even from their own staff.

"In my experience, internal fraud, especially at the senior level, is a real blow for an organisation," he says. "It's embarrassing as it implies your governance isn't great and, because it's about your reputation, rivals jump on that to try and leverage it as an opportunity."

> **"It's embarrassing as it implies your governance isn't great and, because it's about your reputation, rivals jump on that to try and leverage it as an opportunity**

To protect against chief executive fraud, the first, relatively simple, step is to ensure there are policies in place relating to separation of duties, whereby more than one person is required to complete a given transaction, such as authorising payments.

Ceri Charlton, associate director at security and risk assurance services provider Bridewell Consulting, explains: "If two people have to do something, it dramatically reduces the likelihood of misconduct. Typically for collusion to occur, you need a peer to co-operate, who is generally at the same level as you, and overtly asking someone to commit fraud is really quite a big step for most people to overcome."

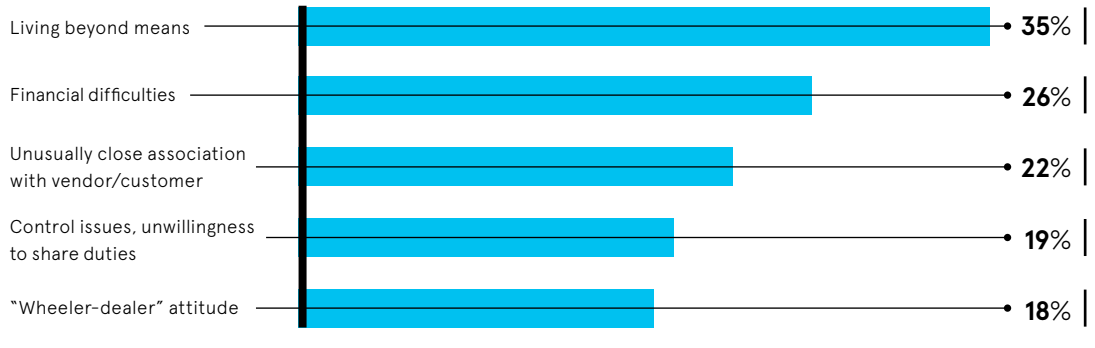
Other reasonably straightforward actions to prevent chief executive fraud include introducing vetting procedures for all senior appointments and ensuring there are adequate controls, compliance programmes and processes in place to investigate allegations of misconduct.

Rather more difficult though is finding ways to change the company culture and its underlying governance to deal with the root causes of such behaviour. As Mr Hernandez points out, misconduct usually results from a combination of a "toxic culture, inadequate oversight and pressure to cheat or cut corners", all of which need to be addressed effectively.

This is particularly true in the case of command-and-control leadership cultures, in which managers and employees alike are usually afraid to question or challenge the status quo.

"Organisations can best protect themselves by fostering a speak-up culture that empowers whistleblowers and encourages dialogue on ethical dilemmas," Mr Hernandez concludes. "But they can also successfully address fraud by regularly assessing risks, communicating expectations for conduct and making necessary changes to excessively risky strategies, practices and business models."

FIVE BEHAVIOURAL RED FLAGS FOR CORPORATE FRAUD



Harvard Business Review 2017

OPINION

‘As we each build our strategies, it can lead us to ask whether creating full protection for digital privacy is even an option?’

As the digital world permeates more areas of consumers’ lives, the degree to which people trust digital devices, services and organisations becomes increasingly important. This has also forced privacy to become a new priority and generated a growing conversation across industries.

On the regulatory side, the implementation of the General Data Protection Regulation in Europe last year drove the issue to the top of the agenda and resulted in similar legislation around the world, such as the Consumer Privacy Protection Act in California.

From a business perspective, several high-profile chief executives have recently commented about importance of privacy. I thought Google chief executive Sundar Pichai put it very well when he noted, "Privacy cannot be a luxury good offered only to people who can afford to buy premium products and services. Privacy must be equally available to everyone in the world."

Given all the technology and resources that industry leaders have access to, it’s interesting to see how something as simple as privacy can raise so many comments, conversations and concerns.

When Money20/20 started in 2012, there was a broad conversation about the impact mobile technology would have across industries. It was changing how people interacted with longstanding companies and institutions, as well as new brands that were arising to implement this technology in a completely new way.

Similar to the momentum and shift that took place around mobile technology, there are now rising broad conversations about privacy that include some of the most powerful and influential people in the economy.

While the wording on public statements, similar to Sundar’s, share a common theme and sound the same, we can speculate that the closed-door conversations on privacy will vary dramatically.

How a company defines privacy, their boundaries and who has the final say are fundamental questions that drive different outcomes. These often vary even within the same organisation as each company has vastly different business models, cultures and histories, each of which comes into play in these conversations.

In reviewing public statements and conversations on privacy, you can get a false sense that the debate is black and white, but in reality we are in the early stages of this long public discourse. Similar to the early days of mobile, conventional wisdom will be flipped and challenge long-held beliefs. There will be many experiments from players entering and exiting the space before we find the few, true long-term winners.

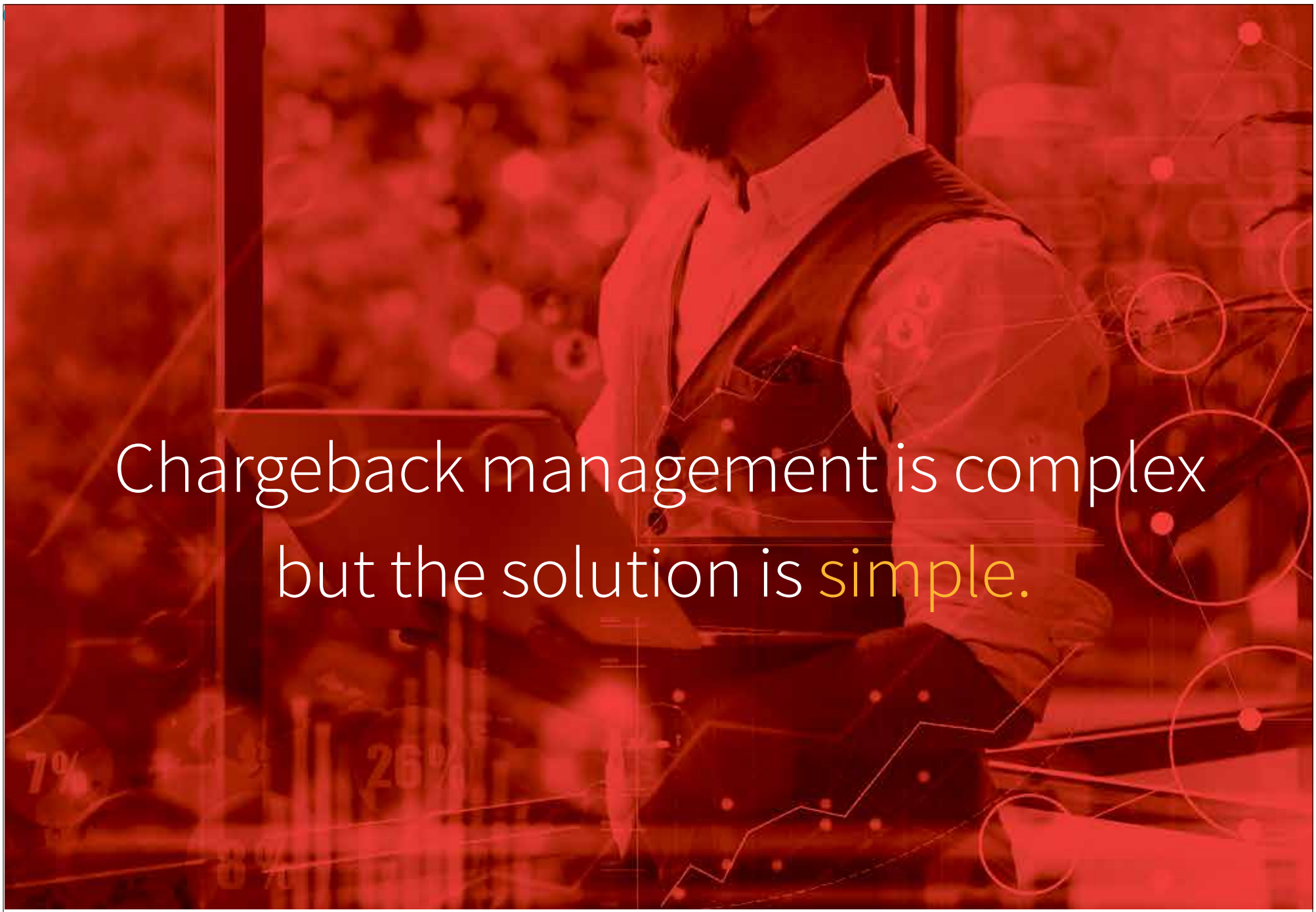
During the early days of mobile, it was important to have a strategy for this emerging platform, which later evolved to mobile first. What we can take from this is the importance of thinking about how you can become privacy first when building your privacy strategy, a process to retrofit privacy on to existing infrastructure.

A privacy-first approach places importance on the experiences we can create, placing privacy as a core tenet. As a rough litmus test, you can compare the results of this thinking with the consumer privacy expectations of each different generation, all of which will have dramatically different views on privacy. This type of thinking can remove the constraints and broaden your strategies, so your company may be one of the few long-term winners.

As we each build our strategies, it can lead us to ask whether creating full protection for digital privacy is even an option? At Money20/20 we’ll be diving into the toughest privacy and security questions, and helping provide actionable insights and takeaways to help you build your privacy strategy, no matter what phase your business is in.

Sanjib Kalita
Editor in chief, Money20/20

Money20/20 USA will be held October 27–30, 2019 at The Venetian Las Vegas. To learn more and attend visit us.money2020.com



Chargebacks are complicated, frustrating, and a drain on your revenue ... but they don't have to be a cost of doing business. Chargebacks911® offers the only **comprehensive chargeback management** solution that can help you identify threats, mitigate risks, and stop losing revenue to chargebacks.

CHARGEBACKS911®
CHALLENGE THE STATUS QUO

2019 CNP 2019 CNP
BEST CHARGEBACK MANAGEMENT SOLUTION
CUSTOMER CHOICE AND JUDGES CHOICE

chargebacks911.com
+44 (0) 2037 505550