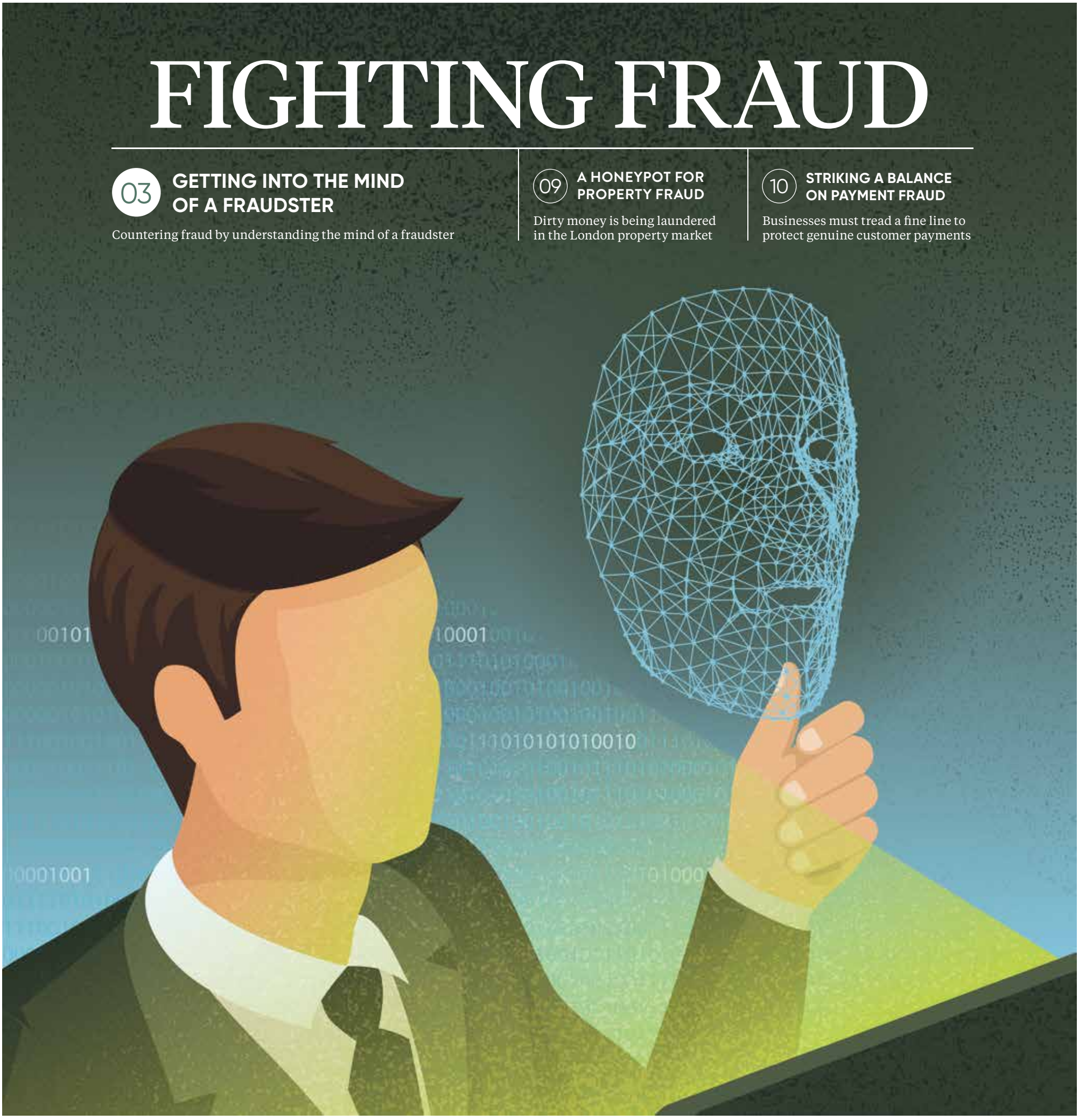
FIGHTING FRAUD



IT and Cyber Security Experts

Blue Cube
Intelligent Protection

Call us today to discuss your cyber security requirements

0345 094 3070

www.BlueCubeSecurity.com

FIGHTING FRAUD

DISTRIBUTED IN
THE TIMES

PUBLISHED IN ASSOCIATION WITH
TRANSPARENCY INTERNATIONAL UK
fighting corruption worldwide

RACONTEUR

PUBLISHING MANAGER
Jack Pepperell

PRODUCTION EDITOR
Benjamin Chiou

MANAGING EDITOR
Peter Archer

PRODUCTION MANAGER
Antonia Bolcas

DIGITAL CONTENT MANAGER
Jessica McGreal

DESIGN
Samuele Motta
Grant Chapman
Kellie Jerrard
Anthony Gerace

CONTRIBUTORS

RICHARD BROWN
Business journalist, writer and presenter, he has worked for leading media organisations in London, New York, the Middle East and Asia.

CHARLES ORTON-JONES
Award-winning health journalist, he writes for national newspapers and magazines, and blogs on health innovation and technology.

LEO KING
Writer and editor, he works with the *Financial Times*, *The Sunday Times*, *Forbes*, *Bloomberg*, *The Economist* and *The Daily Telegraph*.

NICK EASEN
Award-winning freelance journalist and broadcaster, he produces for *BBC World News* and writes on business, economics, science, technology and travel.

OVERVIEW

Getting into the mind of a fraudster

Understanding why people commit fraud is a starting point in countering the heavy losses sustained by businesses

CHARLES ORTON-JONES

"Sun, sea and scams" ran the headline. The story was how families are going on holiday to the Med and then claiming they've suffered food poisoning. A bit of legal work and they get their holiday costs back, plus a nice little compensation payment. Claims are up 50 fold in three years.

It's fraud. But why is the fake food poisoning scam suddenly so popular?

"Fraud is like a water mattress," says Sarah Hill, head of fraud at BLM, an insurance and risk law specialist. "You shift pressure from one zone and it just moves."

In this case the culprits are cold callers. They buy lists of holiday returnees and give them a patter about collecting a pay-off, risk free, if they've been ill. A memory of feeling a bit green after too many sangrias mutates into a claim of full-on gastroenteritis. The cold callers get a slice of the action.

"The holiday-makers think it's a bit of easy cash," says Ms Hill. "Last year, whiplash claims were the chosen scam. When it became clear courts would investigate claims, the cold callers moved to a new space."

This is the world of fraud. Old wheezes are constantly tweaked and repackaged.

The absence of true novelty means we have a pretty clear picture of fraud. We know who the perpetrators are and why they do it.

The "who" is best split into three categories. There are the gullible novices, lured into fraud by a third party or the lure of an easy payment. Often they aren't sure they are committing a crime, merely bending the law in return for a victim-free pay day.

In the second category are the desperate. They need the cash, due to debts, a failing business or other problems. Fraud is the solution.

And third are the criminal gangs. For them, fraud is a way of life.

In each case there are similar mental processes at work. The academic Donald Cressey coined the term "The Fraud Triangle", now the standard model for the industry. This theory says there must be pressure, opportunity and rationalisation. The pressure is the motivation. The opportunity is the chance to commit a fraud; the clear sight of riches can pervert even a steadfast mind. And rationalisation is how we justify our actions to ourselves.

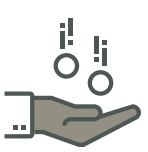
Rationalisation is a fascinating field. Perpetrators rarely see themselves as malefactors. Either they believe they are "owed" a pay day or that the crime is victimless, or they engage a black state of mind to avoid the issue altogether.


Armando Arauz/Unsplash

"Typically, those committing fraud use psychological strategies to distance themselves from any sense of guilt," says Mark Fenton-O'Creevy, professor of organisational behaviour at the Open University Business School. "Criminologists refer to this as 'neutralisation'. A common form of neutralisation is to view the victim as in some way to blame. Another is to depersonalise or belittle the victim. For example, the perpetrators of a series of frauds on eBay referred to their 3,000 victims as 'the idiots'."

For this reason, online and financial fraud are easier to perpetrate. Victims are faceless.

Rationalisation is easier when the origin of the fraud is benign. For example, there is the "thin end of the wedge effect". The offender starts small; usually with something so innocent it barely merits a mention. Slowly the situation requires a little more and a little more, until large-scale wrongdoing is underway.



66%
of corporate fraud was for personal gain and greed

65%
of fraudsters are employed by the victim organisation

21%
are former employees

KPMG 2016

In demographic terms, we have a good idea of which segments of the population are most likely to commit fraud. For example, fraud is gendered. Jonathan Fisher, of Bright Line Law and founder of the White Collar Crime Centre to research aspects of corporate fraud, points to the work of US sociologists Darrell J. Steffensmeier, Jennifer Schwartz and Michael Roche.

"Their research concluded, based on a review of 83 corporate frauds involving 436 defendants, that the 'majority of corporate offenders were male' with less than one in ten being female. Moreover, all 'solo-executed frauds were by men; no cases involve an all-female conspiracy; and all-male groups formed the preponderance of conspiracies'. Furthermore, even in the rare cases of female corporate crime, offending women tended to yield lower gains when compared to male offending," says Mr Fisher.

In corporate fraud, personal crises are the most significant factor. A study by KPMG, called *Global Profiles of the Fraudster*, revealed that 66 per cent of corporate fraud was done for personal gain and greed. Only one in four cases were caused by sheer opportunism.

The study found that the image of a lone fraudster is common, but wrong as 62 per cent of corporate fraudsters colluded with others. And only 35 per cent of colluders do so with an internal party. The majority find an outside accomplice who can complete the deed.

Knowing the mindset of fraudsters means counter measures will be stronger. It also explains why stronger sentences are rarely effective. Some dupe themselves into thinking it's OK. Others are enticed in, unaware of the scale of their misdeeds.

"Having interviewed fraudsters who wanted to give a full admission, they were clearly duped," says BLM's Ms Hill. "Often they were not educated and told they were entitled to something which they weren't."

Are we all potential fraudsters? It's a question for the ages. The Soviet dissident Alexander Solzhenitsyn wrote of his time in a Siberian gulag, watching his fellow inmates struggle to survive: "Gradually it was disclosed to me that the line separating good and evil passes not through states, nor between classes, nor between political parties either – but right through every human heart."

It's why the challenge is so great and why the industry attracts some of the brightest minds. We don't have all the answers and maybe never will.

UNAOIL

Drilling for the truth in oil 'scandal'

Controversy surrounds the dealings of an energy consultancy accused of bribery and corruption involving big-name UK companies


Gilbert UZAN/Getty Images

RICHARD BROWN

Explosive claims of industrial-scale bribery and corruption allegedly orchestrated by Monaco energy consultancy Unaoil Group have ensnared two of the UK's most prestigious blue-chip companies.

An alleged exposé, apparently based on leaked Unaoil e-mails, was first published by Fairfax Media's *The Age* newspaper in Melbourne, Australia and *The Huffington Post* in the United States.

It claims to show cursory due diligence processes in the heavily regulated global oil infrastructure and services sector. It also alleges a staggering, multi-million-dollar "kickback" bonanza system paid to venal government officials. In the coded e-mails, bribes were called "holidays"; a one-day holiday allegedly meant $1 million.

The leaked e-mails are said to show how Unaoil "agents" swayed energy industry contract tenders between 2002 and 2012 to the benefit of their top Western clients in some of the most volatile and economically fragile regions on Earth, including Iraq, Syria, Libya and Iran.

Leading UK FTSE 250 firms Rolls-Royce, which provides powerful generators and gas turbines to the oil and gas industry, and Petrofac, which designs, builds and operates oil and gas facilities, join Germany's Siemens and MAN Diesel & Turbo, Swiss engineer ABB, and Halliburton and KBR, the US energy services titans, among others, in being named in the e-mails.

Originally from Iran, the multi-millionaire Ahsani family controls the Unaoil Group, hob-nobbing with an international business elite in superyacht-stuffed Monaco. In 2006, the family's assets were said to be worth €190 million. It is claimed that shell companies controlled by the Ahsanis in the British Virgin Islands, the Channel Islands and the Marshall Islands are part of Unaoil's operations.

According to the e-mails, Unaoil beguiled Western firms into believing they could not clinch deals in resource-rich regions without its help. Family patriarch Ata Ahsani told *The Age* and *The Huffington Post*: "What we do is integrate Western technology with local capability."

As a result of the allegations contained in the e-mails and other information, in July 2016 the UK's Serious Fraud Office (SFO) announced it was conducting an investigation into the activities of Unaoil, its officers, employees and agents in connection with suspected offences of graft – political corruption – and money laundering.

In the US, the Foreign Corrupt Practices Act Tracker shows eight companies there have announced internal investigations concerning their dealings with Unaoil.

Regarding Rolls-Royce, the e-mails focus on Unaoil's Middle East oil contracts negotiator Basil Al Jarah. He is said to have assisted

Rolls-Royce in winning generator supply contracts from 2003 in Iraq worth tens of millions of dollars. This allegedly included Iraqi government oil official Kifah Numan advising Mr Al Jarah to persuade Rolls-Royce to charge the Iraqi government inflated prices.

In January, after a four-year investigation into corruption and bribery allegations against Rolls-Royce in seven jurisdictions, the SFO agreed to a deferred prosecution agreement (DPA) with the company agreeing to pay a disgorgement of profits of £258 million, a financial penalty of £239 million, plus SFO costs of £13 million. DPAs allow companies to pay a fine and avoid the possibility of a criminal conviction.

Although Unaoil is not named in the DPA statement of facts, the UK High Court judge who ruled in favour of the DPA, Sir Brian Leveson, noted that an analogous agreement between Rolls-Royce and the US Department of Justice "addresses conduct relating to Rolls-Royce and RRESI [Rolls-Royce Energy Systems Inc, sold in 2014] arising from an investigation into its use of an intermediary called Unaoil".

Rahul Rose, senior investigative officer at Corruption Watch in London, says the recent introduction of DPAs, which has helped the SFO to bring faster justice, has also undermined confidence that sufficiently robust sanctions are being imposed in corruption cases.

> Companies can engage in corruption, but escape prosecution by paying substantial sums of money to the government

"In particular, Rolls-Royce's £497-million DPA settlement for paying bribes in seven countries over multiple decades creates the perception that British blue-chip companies can engage in the most egregious corruption, but still escape prosecution by paying substantial sums of money to the government," he claims.

Motivating Business to Counter Corruption, a global survey of anti-corruption incentives and sanctions conducted in 2016 by the Humboldt-Viadrina School of Governance in Berlin, shows fines rank as only the sixth most influential sanction against corrupt firms.

In May 2016, Petrofac engaged lawyers and auditors to investigate claims that a former employee paid $2 million to seal an oil deal in Kuwait. The leaked e-mails claim Petrofac's former vice-president, Peter Warner, urged Unaoil to make confidential payments via a bank account in the Marshall Islands, an acknowledged tax haven. Mr Warner later left Petrofac and in 2014 joined the board of Unaoil.

The same leaked e-mails indicate that in 2008 and 2009 Unaoil promised a middleman €2.75 million to help Petrofac win contracts from the Assad regime's petroleum companies in Syria. Petrofac chief executive Ayman Asfari, who was questioned under caution by the SFO earlier this year, strenuously denies having any dealings with the Assad regime.

It seems Western firms put their faith in the Unaoil Group, relying on anti-corruption due diligence performed on business partners. One such anti-corruption firm that certified Unaoil is New York-based TRACE International. Its president Alexandra Wrage conceded that no due diligence review or compliance policy is a guarantee against wrongdoing.

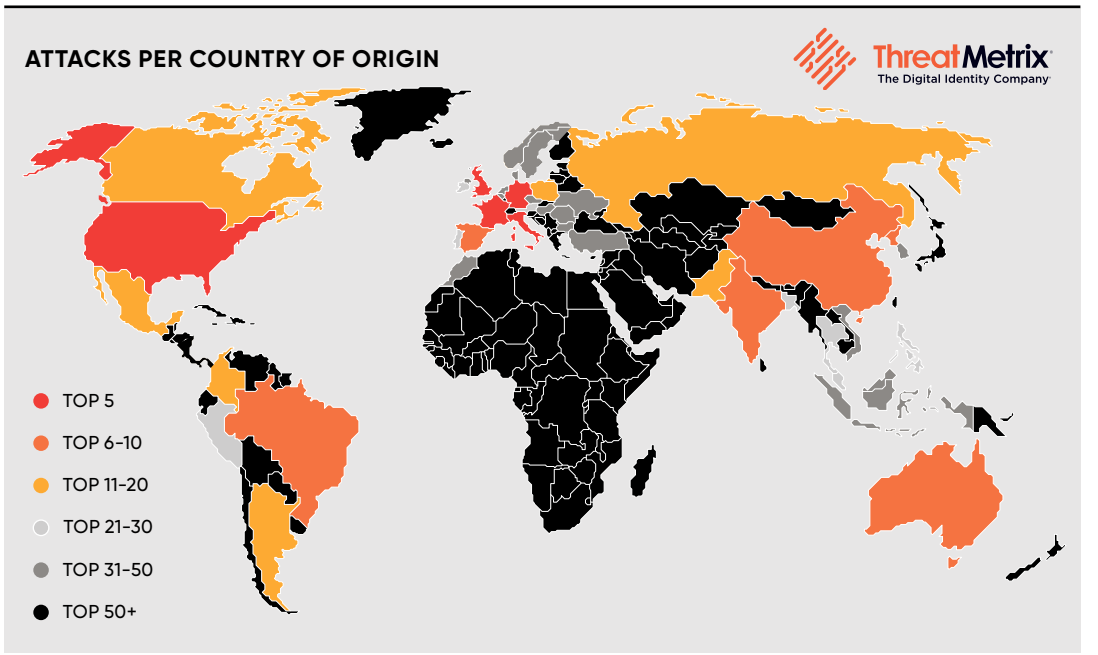
"Compare due diligence to the ISO fire safety standard," she says. "Certification against that standard may well identify risk areas, but it will never guarantee there will never be an accidental fire and it certainly doesn't provide protection against an arsonist."

Ms Wrage claims that Unaoil made material misrepresentations to TRACE International during the due diligence process. Their certification was revoked on these grounds. "While some might find the Unaoil story shocking, the compliance community is rarely shocked by revelations like these," she adds.

The UK Bribery Act 2010 is now among the strictest anti-bribery legislation in the world. It introduced a new corporate offence that placed the burden of proof on companies to show they have adequate procedures to prevent bribery. It also imposes strict penalties for active and passive bribery by individuals as well as firms. Transparency International notes that the Bribery Act has extensive extraterritorial reach both for UK companies operating abroad and for overseas companies with a presence in the UK.

Barnaby Pace, campaigner with Global Witness's oil, gas and mining team, says mandatory payment transparency laws in the EU, US, Canada and Norway attempt to combat the insidious problem of bribery and corruption in the natural resources sector. He explains: "Companies listed on a regulated stock exchange have to now declare what they pay governments for minerals, taxes and licences for every project wherever they are in the world."

Tancredi Communication, Unaoil's public relations consultant, failed to respond to repeated requests for comment. ABB, Halliburton, Siemens and MAN Diesel & Turbo were not immediately available for comment. Jo Rickards, solicitor for Unaoil, says: "We cannot comment at this stage, but we look forward to addressing all the allegations at the appropriate time." ●



Behavioural analysis and digital ID slash fraud

Understanding the real-time behaviour of people online and checking their genuine identity enables proper fraud detection and a seamless consumer experience

This year has witnessed an increase in automated fraud with bots attacking the access and payment rights of millions of consumers. Criminal gangs are obtaining information, then hitting multiple banks, retailers and other businesses. But as companies fight back, they may be concentrating on old-fashioned authorisation and missing the importance of dynamic analysis of customer behaviour.

Typically, automated attackers will take user credentials and test them to access or open accounts. Cyber criminals may also try calling a person, pretending to be conducting a security check and getting them to install software that steals their credentials.

Research by ThreatMetrix, the digital identity company, shows that in the last quarter, most automated bot attacks came from the United States, Germany, China, India, Vietnam, Brazil and Russia. South America became a common location for account origination attacks, while Europe is the key originator of account takeovers targeting bank and online store customers.

ALISDAIR FAULKNER
CHIEF PRODUCTS OFFICER
THREATMETRIX

"With so much personal information on the dark web, people are transacting every day with credentials already in the hands of cyber criminals," says Alisdair Faulkner, chief products officer at ThreatMetrix. "To know what to authorise, businesses have to analyse real-time behaviour and the genuine identity of people trying to access their systems."

ThreatMetrix, which stopped 144 million attacks and 300 million bot attacks in the last three months alone, looks at the transactional devices used, the web browsers or mobile apps, identity information and where users claim to be located. They capture and anonymise data, comparing usage patterns.

"If we see the same device using a large number of e-mail addresses, a flag is raised," says Mr Faulkner. "And if we see that device appearing in the UK when we know it is in Vietnam, there is something suspicious going on." Such factors can be combined with how the user normally transacts, at what times and on what devices or which sort of transactions they favour.

Traditionally, businesses have struggled to block fraud in this way, relying instead on static login passwords that do not spot many of the danger signs and sometimes on laborious authentication steps, requiring additional fobs or tokens for access.

Sellers are at risk of blocking genuine transactions, causing substantial revenue and brand damage. As an example, a user known to have had data stolen and sold on the dark web would normally be asked by a bank or seller to change their password. But each extra step makes a genuine customer more likely to drop out. By using intelligent analysis, a seller can keep processes simple and know whether a transaction attempt was by the account holder.

Financial firms such as Lloyds Banking Group, and apps and websites such as Badoo, are already using ThreatMetrix. Other industries include media and communications, which can check the real location of people trying to stream content.

Such systems balance privacy and anonymity, helping consumers make transactions more easily and quickly, while preventing fraudulent activity. "Consumers want to reclaim their digital identity and privacy while at the same time being better protected," says Mr Faulkner. "Knowing this, there is the opportunity to anonymise and analyse a range of information, enabling billions of frictionless real transactions while protecting against fraud."

Applying such intelligence allows online businesses to recreate the personal and easy buying experience that bricks-and-mortar firms thrive on. Mr Faulkner explains: "You go into a store expecting a service, not to have to jump through hoops. It's the same with digital identity, ultimately you can be safe and get the services you want, with one click instead of many."

To find out how to use digital identity and behaviour analysis to secure your customers and ease transactions please visit threatmetrix.com

OPINION COLUMN

‘As the UK prepares to leave the EU, we can’t afford to leave our defences against corruption waiting in the wings’

ROSE ZUSSMAN
Campaigns officer
Transparency International UK

Too often the debate about corruption has people exclusively looking beyond these shores, but as preparations for Brexit continue, we cannot afford to forget that corruption happens every day – and it is happening in the UK.

Ask the police officers who had to arrest their own colleagues for money laundering. Ask the 41 per cent of construction workers who have reported being personally offered a bribe. Ask someone working in a prison.

Ask anyone from the countries around the world where funds for healthcare, education and infrastructure are siphoned off by public officials, laundered through the Overseas Territories, and then used to buy properties in central London.

In the case of the Grenfell fire tragedy, which has sparked questions around whether corruption might have played a role, it is far too early to tell. But in similar disasters in other countries – those in which the incredible loss of human life is perceived or understood to be a direct result of shoddy construction work – questions about the involvement of corruption are often the first asked.

The UK must in equal measure cover all its bases in the Grenfell Inquiry, given the number of known corruption risks in construction, local government and procurement.

Corruption isn’t a problem we have in epidemic proportions, but there are essential areas the UK has yet to get a grip on. Our concern shouldn’t be reserved for when shocking stories make the news. We have to step up to plate now and for the long term, especially as we prepare for Brexit.

Disentangling European Union and UK legislation, a process experts believe may take up to a decade, and one which may leave little room to ensure our anti-corruption laws are up to date, will find us more reliant on the quality of the UK’s own political systems.

We must consider and amend the robustness of these systems, with 39 loopholes in the lobbying rules that open the door to corrupt activity.

Equally, as we venture into emerging markets, where in many cases there is perceived to be a higher prevalence of public sector corruption than in most EU countries, the levels of risk faced by UK exporters could increase. In looking to retain the UK’s reputation as an attractive place to invest, we may be less likely to turn away undesirable partners, potentially exacerbating the use of the UK as a place to hide stolen money.

These scenarios are far from ideal, but Brexit need not mean corruption worsens in the UK. There are at least three measures the UK can take now to prevent it being used as a safe haven for the corrupt.

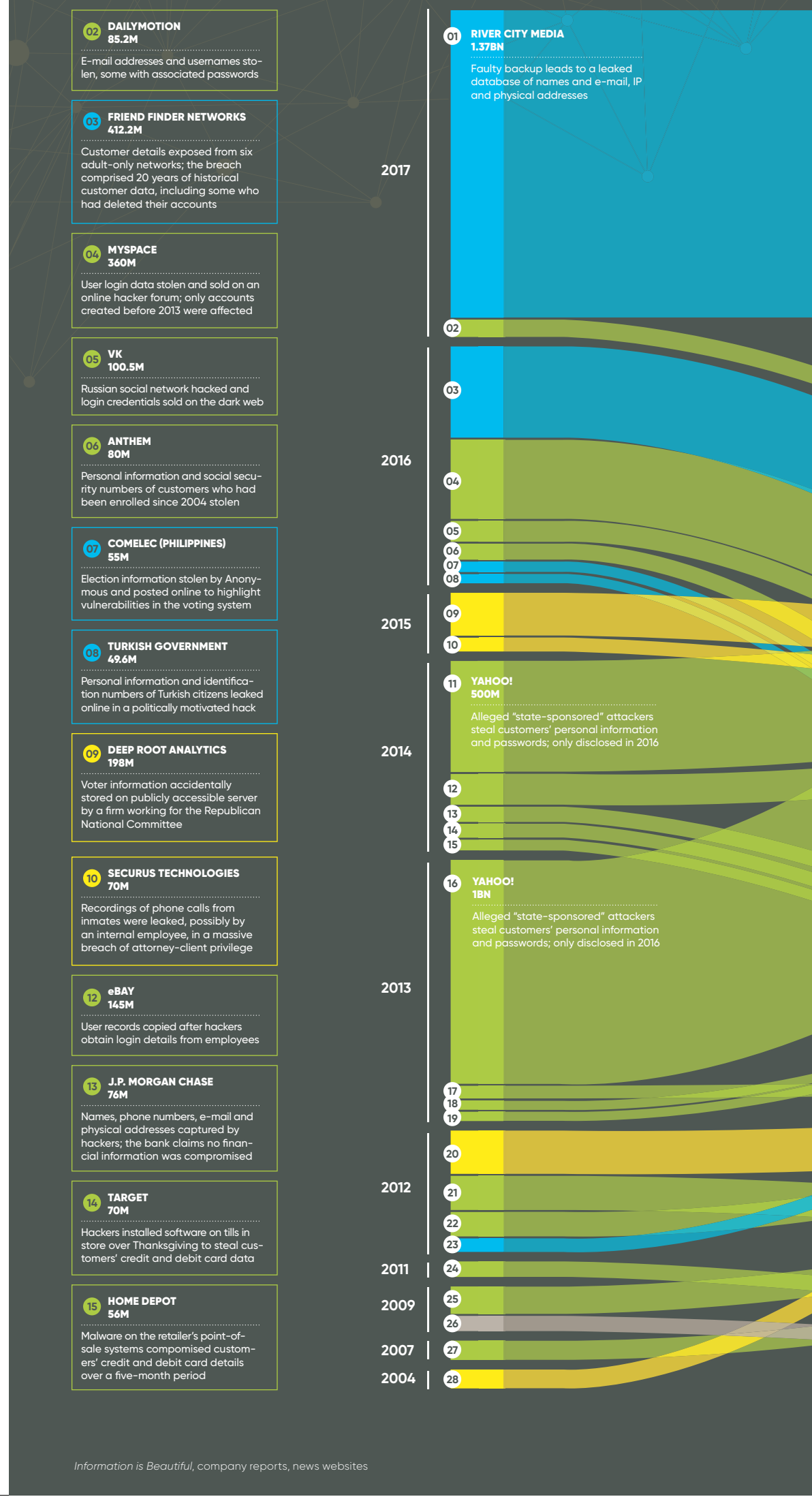
Firstly, we need to build anti-corruption provisions into our post-Brexit trade agreements, resisting temptation to attract inward investment on a no-questions-asked basis, and introduce greater transparency around the lobbying of government and Parliament.

Secondly, there need to be greater efforts to prevent money laundering through UK property. In London alone, Transparency International was able to find £4.2-billion-worth of property bought with suspicious wealth.

Yet we are still waiting for the government to deliver on its promise to introduce more transparency around the real owners of overseas companies that are buying UK property. The government committed to have a new law in place by April 2018, but questions are being raised around whether it is serious in its efforts. The Queen’s Speech made no mention of this legislation which will need enough time to progress before Brexit.

Finally, the government must urgently launch its long-awaited anti-corruption strategy, now well past its 2016 deadline. This should provide a framework for countering corruption with a clear set of objectives and a long-term vision that will take us through Brexit, and well beyond.

DATA BREACHES



Information is Beautiful, company reports, news websites

From the United States military to the Filipino government, data breaches can affect companies, public-sector agencies and organisations of all types. This infographic charts some of the most notable hacks in recent history, how they happened and how many records were breached

TYPE OF FRAUD

- Hack
- Insider job
- Leak
- Lost/stolen media

COMPANY/RECORDS BREACHED

17 TUMBLR 65M

Personal information from user accounts was stolen and put up for sale on the dark web; the hack was not revealed until 2016

18 EVERNOTE 50M

Company resets passwords of every single user after hackers gained access to usernames, e-mail addresses and encrypted passwords

19 LIVINGSOCIAL 50M

Hackers steal login credentials of user information from the majority of the website's customers

20 COURT VENTURES 200M

Vietnamese national poses as client and steals personal, financial and social security data of millions of Americans

21 MISCELLANEOUS 160M

Hacking ring steals credit and debit card numbers from banks, payment processors and retail chains over eight years

22 LINKEDIN 117M

User credentials hacked and sold on the dark web

23 DROPBOX 68.7M

Users' e-mail addresses and passwords were stolen in 2012, and then leaked on hacker trading sites in 2016

24 SONY PLAYSTATION 77M

Week-long network outage occurs after an "illegal and unauthorised person" obtains gamers' personal information

25 HEARTLAND 130M

Hackers steal the digital information encoded on to magnetic strips of credit and debit cards, allowing them to fashion counterfeits

26 US MILITARY 76M

The National Archives and Records Administration sent a defective, unencrypted hard drive for repair without first destroying the data which included veterans' social security numbers dating back to 1972

27 TK/TJ MAXX 94M

Hackers breach retailer's Minnesota store wi-fi to steal credit and debit card information

28 AOL 92M

Former software engineer sells customer information to spammers who sent out billions of e-mails marketing penile enhancement products

COMMERCIAL FEATURE

New data security laws are coming – are you ready?

Careless paper disposal now commands record fines, yet most companies are in the dark, says **Neil Percy**, vice president of market development at **Shred-it** in Europe, Middle East and Africa

At some point we are going to see signs of panic. But not yet, apparently. The biggest change in data security for a generation is almost upon us and the bulk of businesses are disconcertingly unaware.

A recent survey conducted by Ipsos for our company Shred-it examined UK companies' readiness for the European Union's forthcoming General Data Protection Regulation or GDPR. The results were worse than we had anticipated.

Eighty-four per cent of UK small-business owners and 43 per cent of senior executives at large companies are unaware of the GDPR.

The numbers who knew the penalties for breaching the regulations were worryingly low. Only 14 per cent of small businesses and 31 per cent of executives at larger companies understand that the penalties can reach up to €20 million or 4 per cent of global turnover.

The GDPR comes into force across the EU in May 2018. In a nutshell, vast swathes of UK companies are approaching this date unprepared and the implications if they don't act soon are significant. Ignorance of the law, as they say in legal circles, is no defence.

WHAT THE RULES DEMAND

The GDPR imposes enhanced obligations around data management for companies of all sizes. For example, when being asked for their consent, individuals will be required to be given a far more detailed understanding of how their data will actually be used. If they want data destroyed through the right to erasure, this may be requested and must be executed without fail. A data protection officer may need to be appointed and data breaches must be reported to the regulator, the Information Commissioner's Office, within 72 hours. No buying time to spin the story as delaying could risk increased penalties.

The message is clear. Every organisation should look to develop a comprehensive data security strategy. However, one area of disconnect in particular stands out. Where electronic data is concerned, most companies already have a strategy with developed protocols, passwords, access controls and other security measures. The gap is often in the treatment of physical data for disposal. Letters, financial records, reports and other printed confidential materials are often treated as low risk or worse considered as waste rather than as a security concern. Documents are either intentionally or accidentally sent for recycling, or simply dumped in the bin, with no thought of their destination or who may access that information once in process.

> Letters, financial records, reports and other printed confidential materials are often treated as low risk or worse considered as waste rather than as a security concern

Under the GDPR, the risk from this oversight is heightened. Personal data in any format, electronic or physical, falls under the regulations. Printed confidential data must therefore be considered integral in forming the security strategy, treated with equal concern as that afforded to digital data.

Use of small office shredders is often a chosen solution for some organisations. While this may meet the intended security protocol, it is often limited by the time employees have available or simple elements, such as paper clips, plastics or laminates that are problematic for the machine, and all too often users resort to recycling or waste disposal. In effect, a paper clip can break the security system.

This means that even when companies try to comply in-house with the GDPR they may struggle.

HOW TO REACT

The solution is to seek the advice of a dedicated specialist. This is the domain of Shred-it. We are the UK and global leader in document destruction. In the UK we serve 35,000 customers from 18 service centres, destroying more than 5,000 tonnes of confidential paper on average each month.

Last year our certified information security professionals carried out 5,000 workplace data security risk assessments in the UK alone, helping organisations of all sizes understand their security risk.

We bring three unrivalled qualities to the job. Firstly, we will develop a bespoke solution that will review current process and recommend any areas of improvement in the capture and secure handling of confidential information for disposal. Secondly, we help you build a secure process for destroying physical documents and data within the GDPR's fundamental spirit of "privacy by design". Thirdly, we bring a raft of service options. Our destruction services may be conducted at your premises or off site at one of our service centres, on a regular basis or on demand, depending on your needs.

Shred-it can also assist in electronic media destruction ensuring hard drives are physically destroyed from redundant computers, servers and flash drives, rendering data unrecoverable.

Shred-it's international profile sees our reach extend across 21 nations helping more than 400,000 businesses worldwide achieve the highest level of rigour in their security policy. Multinationals know they can use Shred-it and get the same gold standard of service, in keeping with security policies across multiple markets.

The result of partnering with Shred-it is that companies can give confidence to investors, customers, commercial partners and regulators that they have a fully rounded, auditable, strategic security process around the destruction of all forms of personal and confidential data. This is no small thing. Data breaches have cost companies a fortune in the recent past. Aside from penalties incurred, the reputational damage to the company can be severe.

COST OF FAILURE

Inaction may mean violating the GDPR. That exposes organisations to the risk of reputational damage and financial penalties. We can also expect customers to ask their suppliers for guarantees around the protection of shared data, including the handling of printed data. If suppliers cannot provide those guarantees then customers are likely to consider other options.

Conclusion? Before May next year, companies will need to review current processes and conduct in-depth audits and risk assessments in light of the new regulations. An industry specialist can help with this. Legal advice should also be taken. In addition, training staff will be essential.

Above all, companies need to know and prove that all confidential information, regardless of format, is effectively secured.

As the rules get tighter, the importance of working with a specialist will only grow.

To find out more please visit shredit.co.uk/gdpr

LACK OF AWARENESS LEAVES UK BUSINESSES AT FINANCIAL AND REPUTATIONAL RISK

Shred-it Information Security Tracker 2017 powered by Ipsos

FIVE KEY CHANGES UNDER THE GDPR

01 All personal information, regardless of format, falls under the GDPR.

02 Public authority bodies and companies which process large volumes of personal data will need to appoint a nominated data protection officer.

03 There will be stricter rules around securing consent to use personal information, and businesses will need to show they have a definitive agreement from individuals to collect and hold their personal information.

04 The right to be forgotten will be introduced as standard.

05 Data processors, companies or individuals who support and supply data controllers, will also be regulated.

MONEY LAUNDERING

London: a honeypot for property fraud

Dirty money is being laundered in the London property market by criminals hiding behind anonymous shell companies, pushing up prices beyond the reach of ordinary Londoners

Simon Dawson/Bloomberg via Getty Images

Kensington has the highest density of unoccupied housing in London

NICK EASEN

Wait until dark, then walk down some select streets in London's Kensington and Chelsea and you'll be aware that it's eerily quiet. Peer into the houses and you'll notice few lights on. Not many people are at home and the others are not out revelling – there's a good chance the owners are overseas.

While many in Western Europe's largest city struggle to find affordable housing, nearly 20,000 houses worth more than £9 billion were unoccupied in 2016 and the highest density was situated in Kensington, according to a study by Property Partner.

That's because London's bricks and mortar are still one of the most sought-after commodities for global investors, particularly in the wake of the post-Brexit tumble of sterling. However, there's a dark underbelly to this and overseas corruption could be pricing Londoners out.

To date, empty homes are a major conduit for laundered money, according to Transparency International UK. The numbers are astounding as £4.2-billion-worth of property in the capital may have been purchased with the proceeds of suspicious dealings.

Tot it up and 40,000 properties are registered to owners who've hidden their identities behind anonymous, shell companies, sitting in the likes of Jersey, the Cayman Islands or British Overseas Territories. Transactions are even masked through multiple offshore jurisdictions.

£4.2bn

worth of properties in London may have been bought by high-corruption risk individuals

Transparency International UK 2017

"This enables corrupt individuals to buy houses in secret without law enforcement agencies, regulatory bodies or the general public knowing who they are," says Duncan Hames, director of policy at Transparency International UK.

The previous government committed to a public register identifying people behind overseas companies that own UK property. However, it's unclear whether this legislation will be included in the upcoming parliamentary session.

The British government estimates that £100 billion is laundered through the UK each year. Since London is at the centre of a sprawling financial network spanning the globe, it's not surprising that property is used as a fraudulent asset class, but what is remarkable is how much goes unnoticed.

Only 335 out of some 1.2 million property transactions in 2015 were deemed to be suspicious, according to the Commons Home Affairs Committee last November. It doesn't help that many banks are unwilling to question the source of funds and don't adopt a "guilty until proven innocent" stance over such issues.

"The longer London, including both the government and private sector, does nothing, the tougher the trend is to reverse," says Tom Keatinge, director of the Centre for Financial Crime and Security Studies at the Royal United Services Institute.

"What we now need is a 'shock and awe' campaign. If the UK wants to clean up its act, then it needs to act with purpose. Interviews that I've done in Central Asia about perceptions of the UK are almost unanimous in their agreement that the rhetoric about dirty money emanating from London is just that and nothing more, rhetoric."

Minor changes have been made to money laundering regulations. These now state that estate agents must conduct due diligence on buyers. Before, they just had to do this on sellers. It's hardly revolutionary, though.

"Before this was in place there was a danger that different professionals involved in these transactions were relying on each other to carry out money laundering checks, resulting in corrupt individuals slipping through the net," says Mr Hames.

The Criminal Finances Act comes into force in the autumn and should change things, enabling the authorities to target property purchased with suspicious wealth by issuing unexplained wealth orders or UWOs.

Those with questionable assets will have to explain the source of their wealth and, if inadequate answers are given, property can be seized.

> Those with questionable assets will have to explain the source of their wealth and, if inadequate answers are given, property can be seized

"Law enforcement agencies will need to make sure UWOs are used to target property specifically. To help with this process and deter money launderers in the future, we do need this public register to identify who's behind these overseas companies," says Mr Keatinge.

The biggest losers in this are Londoners. Some developers in the capital already cater directly to overseas investors, who will buy at the higher end of the market, neglecting the needs of locals when they're building.

In a recent survey of 14 new landmark developments, worth £1.6 billion, four out of ten homes had been sold to investors from high-corruption risk countries or those hiding behind anonymous companies. Less than a quarter were bought by UK buyers.

"We cannot legislate ourselves to a better place. We have to take action and that requires resources, commitment and backbone, three ingredients in short supply unfortunately," Mr Keatinge concludes.

Proactive approach can secure business payments

Business payment fraud is not just a growing problem, it's a mutating one

Bottomline Technologies

A challenge for organisations is that the pace of change is accelerating so only a holistic strategy and a comprehensive set of defences can secure how they pay and get paid.

Five years ago, payments took much longer to complete than they do now, perhaps three days for a transfer. The upside of this delayed time allowed chief financial officers (CFOs) the opportunity to uncover anomalies and call a halt to dodgy dealings before money disappeared.

Today, almost half of UK businesses have adopted the Faster Payments Service, which greatly improves efficiency, but has closed the window in which money can be clawed back.

"CFOs and corporate treasurers can no longer rely on clearing cycles as a buffer to deal with fraud," explains James Richardson, head of market development, risk and fraud, at Bottomline Technologies.

"Criminals have learnt smart ways to catch out organisations, whether it's finance or treasury departments. Yet, the window of opportunity to close them down has shrunk massively."

New frauds are accentuating the problem. Business e-mail compromise, in which criminals posing as the chief executive request immediate settlement of funds, is relatively new, but costs the global economy billions of pounds each year.

"Fraudsters treat this like a business," adds Mr Richardson. "They do research and have 'sales and marketing teams' which probe organisations of all types and sizes for vulnerabilities.

44%

of UK businesses have adopted the Faster Payments Service, reducing the window to clawback payments

42%

of UK organisations don't use technology as part of their payment compliance processes

"E-mail scams are a bit like telemarketing. Chief executives and finance directors are tracked on social media, particularly LinkedIn, and if anyone responds it's as if they are self-selected for a fraud. The sums can be huge, for example an acquisition-related payment, so we're talking millions."

Fake invoices and vendors are just a small part of a much wider problem. Mr Richardson likens it to a balloon, which when squeezed in one area expands in another. It's strong evidence that a "people and process" approach to combating fraud is no longer adequate.

Bottomline is at the sharp end of a change in attitude towards securing business payments. It is repositioning its stance from simply making solutions available to strongly recommending a suite of technologies that can shield financial institutions and corporates.

"New regulatory and security demands, specific to payments, are being mandated for banks and large enterprises," says Mr Richardson. "Currently fraudsters are ahead of the game so organisations should not wait until security becomes mandatory. Instead they need to continuously secure their payments effectively by applying these standards now."

Research by Bottomline suggests more than two fifths of UK organisations don't currently use technology as part of their payment compliance processes. In other words, they rely purely on staff members to raise the alarm if something looks wrong.

> Bottomline is at the sharp end of a change in attitude towards securing business payments

Mr Richardson's advice is to adopt technology that deals with the latest threats. If your thinking hasn't changed in the last three years, he suggests, your business is vulnerable.

"Don't stick with what you have done before; it's vitally important to keep pace with the payment security landscape and emerging threats. Now is the time to think differently.

"Our advice is to look at what security standards and obligations are coming your way, even if they are currently optional or advisory. Don't wait for it to become mandatory; if it makes sense then do it now," says Mr Richardson. "As new threats emerge, new standards will need to be met so organisations must keep up with the pace of change."

Most important is to switch from a reactive to a proactive stance, one capable of monitoring behaviour and detecting payment anomalies before they leave your organisation.

"Having a suite of solutions that looks at the problem from every angle, for every single transaction, is the standard for securing business payments in 2017," Mr Richardson concludes.

For more infomation please visit www.bottomline.com

Striking a balance on payments

Businesses must tread a fine line to protect customer payments – stopping sophisticated fraudsters is crucial, but to avoid blocking real transactions requires a more co-ordinated effort

LEO KING

There is no denying the brutal impact of payment fraud, with $9 billion of annual criminal spending on US payment cards alone, according to research firm Javelin. Nearly six in ten information thefts studied in *Verizon's Data Breach Investigations Report* involve payment details. Meanwhile, in-person card skimming continues to grow, with the last year witnessing a tripling of illegal reader installations at the new weak point, petrol pumps.

Cyber criminals continue to advance and merchants are taking aggressive action to counter them. But businesses' assertiveness also leads them to decline swathes of real payments erroneously.

To balance their fightback, retailers must understand criminals' tactics. A common fraud is social engineering, according to trade association the Merchant Risk Council, and it involves the deception of individuals so they hand over sensitive information.

Phishing is its most common form in which fraudsters amass information over messages, such as fake e-mails or websites from a bank, retailer or payment processor. Sophisticated cyber criminals engage particularly in spear phishing using highly targeted e-mails that include accurate information.

Tim Ayling, European director of fraud and risk intelligence at technology firm RSA Security, warns that fraudsters "will learn anything and everything about their victims – their address, daily routine, even the name of their kids' school teacher". He adds: "All of this is with the end-game of getting them to share bank details or even transfer money directly to accounts."

> More likely than not, fraudsters won't consider prices, read product reviews or look for discount codes

Breaches involving e-commerce sites typically entail the "fairly straightforward process" of hacking a web application to steal logins, explains Laurance Dine, managing principal of investigative response at Verizon. Meanwhile, card skimming dominates in bricks-and-mortar retail.

Companies are aggressively trying to block such theft and in doing so they often inadvertently kill masses of genuine transactions. The revenue consequences are dire. Javelin notes that $118 billion is lost by US retailers every year through false declining, more than 13 times the value of card fraud. And then there is the effect on brand reputation as more than one third of incorrectly blocked people decide to dump the retailer or their card.

This means stores and card issuers "must toe a fine line between protecting their assets and retaining customers", explains Emma Cloninger, marketing co-ordinator at the Merchant Risk Council. She warns that merchants and issuers can easily overreact.

The danger of customers feeling "let down or even humiliated" by a payment decline and then airing their experience on social media, Mr Dine says, means businesses have to be careful. He adds: "In today's hyper-competitive retail landscape, there will always be another retailer out there waiting to swoop up any disappointed or disenfranchised customers."

Merchants are wisely turning to behavioural analytics and pattern spotting to improve their checks. "As a crude example, if a customer has made a transaction in Britain in the morning and then attempts to make one in Australia later that

CHUYN/Getty Images

day, a flag is raised and further authentication is required. Then there are much more granular metrics to confirm that customers are who they say they are, such as the device used, payment method, IP [internet] address and the size or type of purchase," Mr Ayling says.

Payment processor Mastercard is one firm monitoring patterns. Its fraud detection system, Digital Intelligence, "analyses and learns from consumers' transactions, feeding this data into an intelligent network", according to Ajay Bhalla, president of global enterprise risk and security at the company.

The data includes retailer and card issuer information. "From this we're able to improve the customer experience by reducing the number of false declines, while preventing fraudulent transactions from being approved. In essence, we're moving from managing fraud to managing better decisioning at the outset," he says.

Ms Cloninger says retailers must also analyse how people behave on their sites. "More likely than not, fraudsters won't consider prices, read product reviews or look for discount codes," she says. "They'll be in and out within a matter of minutes."

Human judgment must remain an essential partner to this automated analysis. "Though artificial intelligence and machine-learning are excellent all-round tools, they are only tools," Ms Cloninger says. When properly managed and maintained by humans, they improve fraud prevention. And for in-store or petrol pump fraud, where skimmers can be installed within seconds, it is essential humans monitor surveillance footage carefully.

Cross-sector human co-operation is also essential. "Collaboration and data-sharing isn't an option, it's a must," says Mr Ayling. Ongoing discussions have shown a cyber criminal will typically use the same device and tactics when attacking in different countries. He adds: "Not sharing information across borders is only helping the fraudsters."

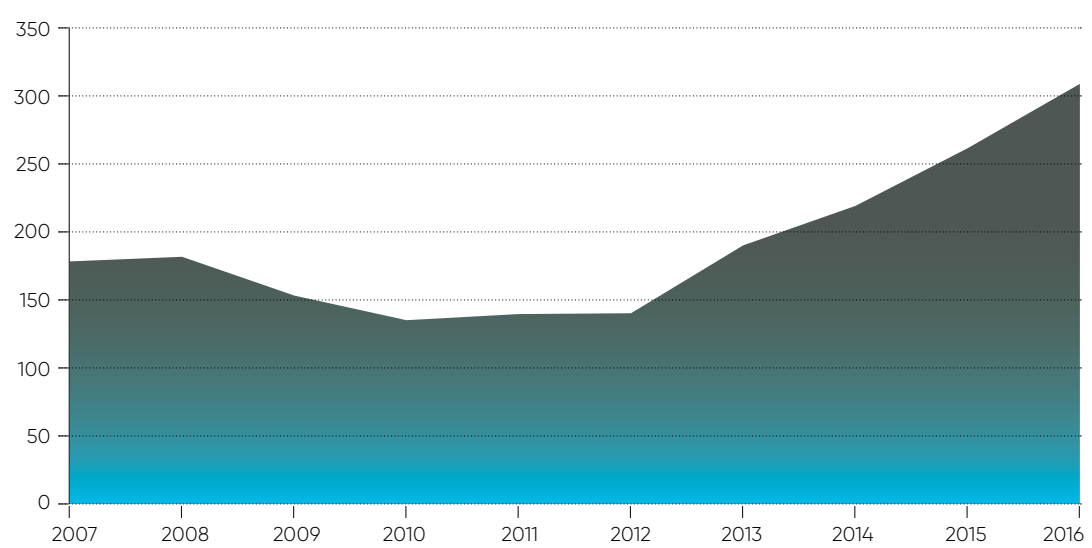
By working together, businesses can reduce fraud and keep the buying process smooth. Companies already discuss confirmed fraud information and there is the potential to assess deeper information on global transaction patterns collaboratively.

US research from Mastercard and the Fletcher School at Tufts University, called the *Digital Evolution Index*, reveals the true potential of international assessments. Countries advanced in digital development tend to lead fraud detection and Mr Bhalla says this is because "those with digital payments operate on a borderless business model, making payments more convenient and fraud easier to detect".

As companies look to become smarter in their fraud detection, they must ensure their innovation is more collaborative. "Fraudsters are consistently evolving, exploring new attack strategies and developing tactics to expose vulnerable targets," Ms Cloninger concludes. It is only through co-operation that businesses will stay ahead of the crooks.

UK ONLINE/E-COMMERCE FRAUD LOSSES (£M)

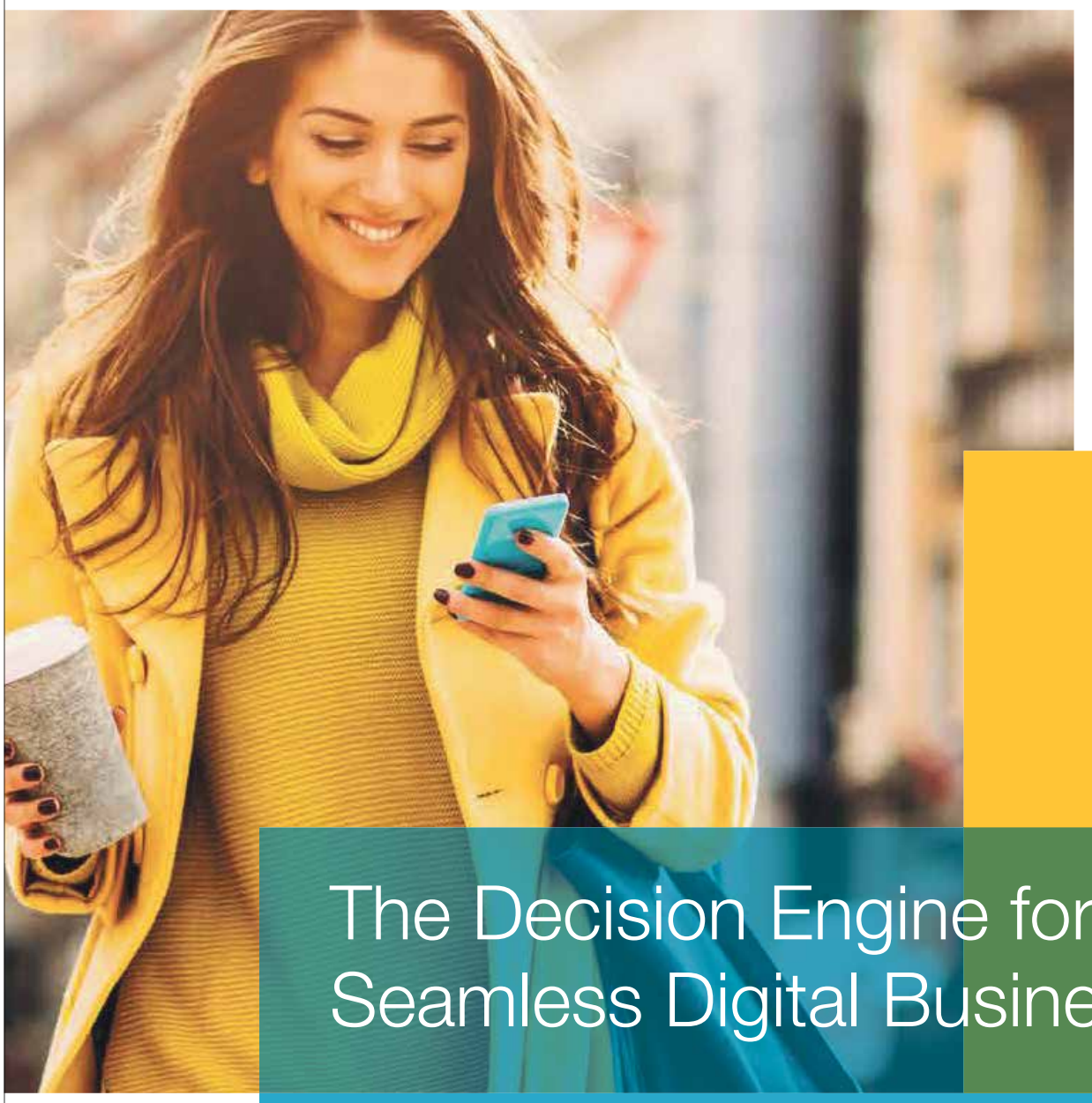
FRAUD LOSSES ON UK-ISSUED CARDS



Financial Fraud Action 2017

ThreatMetrix®

www.threatmetrix.com



The Decision Engine for Seamless Digital Business

Fighting fraud with digital identity intelligence from billions of transactions and a powerful decision platform.

ThreatMetrix Digital Identity Network®

Harness the power of global shared intelligence from the largest network of its kind.

24b	1.4b	4.5b	.8b	1.5b	185
annual network transactions	unique online identities	unique devices identified	unique email addresses	mobile devices	countries served globally