FRAUD FUTURES

Understanding
the OLD
to prepare for
the NEW

FRAUD
ADVISORY
PANEL

FRAUD FUTURES

Fraud, in the widest sense of '**deception for gain**' is as old as human society.

Nor is there anything new and unexpected about the way new technologies empower the fraudster along with the rest of us. It happened with money and the earliest financial products, then the telegraph, the railway and the telephone, all long before the internet dismantled our fraud defences.

So why are we still so bad at seeing fraud coming and trying to design it out of our great innovations?

That is the question at the heart of this special report. It's not an easy question to answer but it is time for all of us – in business, politics and wider society – to ask it with the utmost seriousness.

A chronology of cybercrime

The timeline that runs across the bottom of this report shows various types of cybercrime, arranged by the approximate date they first became apparent according to contemporary reports by the police, courts, media and cybercrime specialists. Each crime type continues to this day, although often in modified form. Telegraphic interception, for example, can now be done remotely and wirelessly.

New cybercrimes follow on from new technologies. Telecommunications technology was first created in 1837 and, as the graphic shows, the earliest illegal interception occurred 30 years later. The widespread use of computer networks brought money laundering and hacking offences. More recently, the introduction of the internet in the late 1980s made it easy to infringe copyright and to distribute offensive material internationally. The latest forms of cybercrime use wireless and mobile technologies and employ encrypted communications in the 'dark web' and the cloud. The very latest biometric and blockchain technologies are already being targeted and the hacking of virtual currencies and IoT (internet of things) devices has begun.

1867 Interception

1850 1900

A short history of fraud

‘Corruption, embezzlement, fraud, these are all characteristics which exist everywhere. It is regrettably the way human nature functions, whether we like it or not.’

Alan Greenspan, chairman, US Federal Reserve (1987-2006)

Tetradrachm of Athens, IV century; left: **Head of Pallas Athena;** right: **Owl and legend ATHE (Athens)**

Where to begin with a short history of fraud? One could easily have framed the subject ‘a short history of mankind’. Ever since Homo sapiens emerged 200,000 years ago there has existed a very human desire to lie and deceive.

Any history of fraud, brief or otherwise, must first define the nature of the act. Put simply, fraud is an intention to deceive for financial or personal gain. It should not be confused with dishonesty for other reasons – such as lying to a friend to protect their feelings – and nor should it be confused with folly.

> While the literal definition of ‘fraud’ can describe a vast range of dishonest behaviours, in practice its application has vexed societies across the ages. How often is the term ‘sharp practice’ applied to what is undoubtedly a criminal fraud? We see this ambiguity played out today in the creation of, say, fake online product reviews which are clearly intended to deceive for financial gain but which are passed off as a regulatory rather than a criminal matter.

Although no definitive accounts exist, the widespread practice of fraud is likely to have emerged during the development of barter as a means of economic exchange. Bartering was first recorded in Egypt in 9000 BC and hieroglyphics of the time show that it often led to violent arguments. It’s easy to imagine one party failing to check the contents of each grain sack exchanged for a cow only to find, on reaching home, that one sack is half empty. More certain is that deceptions relating to barter were commonplace during the period of the Old Testament. The Book of Proverbs, written between 700 and 400 BC, contains many such references:

‘Unequal weights and unequal measures are both alike an abomination to the Lord.’
Proverbs 20:10

Coinage

The next major step-change in human economic development, the introduction of currency, greatly expanded opportunities to commit fraud. The first known currency was created around 600 BC in Lydia, now part of Turkey. The coins, bearing the head of a lion, were irregular in shape and size and made from a naturally occurring mix of gold and silver called electrum. A common practice of the time – and repeated throughout history – was to shave the edges of a coin, known as clipping. The fragments were then used to produce a new coin. ‘True’ counterfeits also emerged around this time, in which a cheap base-metal was plated with the appropriate precious metal.

Trade finance

The rise of the Greek civilisation provided yet more opportunities for fraud. The widespread use of coinage enabled more sophisticated commercial arrangements to develop, including trade finance. The case of Hegestratos in 300 BC, often cited as the first recorded example of fraud, demonstrates the inherent weakness of early commercial contracts. Hegestratos, a Greek sea merchant, abused a system of trade finance called ‘bottomry’ in which a ship and its cargo is used as security for a loan which does not have to be repaid if the ship is lost at sea. Hegestratos, having purchased a policy based on a full load of corn, set sail with his vessel empty, intending to sell the grain separately and sink the ship to escape the debt. Unfortunately for Hegestratos he was foiled by the ship’s suspicious crew.

‘When predicting where frauds are likely to appear in the future we would be wise to track changes in commercial practices (such as the rise of the ‘cashless society’), new technologies (such as artificial intelligence), and the groups likely to wield power in the latter part of the 21st century.’

Oliver Shaw, detective superintendent, City of London Police

Corruption

As the Greek Empire gave way to the Roman Empire the growing acceptance of financial transactions in lieu of the physical exchange of goods further enlarged opportunities for fraud. In 193 AD the empire witnessed a very public investment fraud. The Praetorian Guard, having assassinated the Emperor Pertinax, dishonestly announced their right to appoint the next Roman emperor, the position to be awarded to the highest bidder. Didius Julianus won the auction with a pledge of 250 pieces of gold for every soldier in the army. However, the fraudulent scheme soon unravelled and Julianus, having never been formally recognised as emperor, was himself assassinated in the third month of his reign.

The Roman period also gave rise to the practice of forging art. Replicas of well-known Greek sculptures were made in great quantities to satisfy demand from wealthy collectors. There are no definitive records to suggest that these artefacts were passed off as originals – unlike famous cases of art fraud across the centuries – but this does demonstrate how opportunities for fraud follow the creation of new markets in high value and desirable goods.

Paper money

Very few accounts of fraud are recorded during the remainder of the first millennium. While there were huge advances in technologies such as printing, methods of commercial transacting remained static. Indeed, it was not until the 13th century that opportunities for fraud increased again with the development in China of the first paper currency. Early notes, manufactured from the wood of the mulberry tree, were subject to counterfeiting, leading the government to introduce the death penalty for counterfeiters and to station guards around mulberry forests.

Although crude forms of paper money circulated in Europe from the mid-17th century, it wasn't until 1661 that the world got its first true 'bank note'. Sweden, a banking pioneer to this day, began issuing credit notes – *kreditivsedlar* – underwritten by the Stockholms Banco institution. The notes could be exchanged for a stated number of silver coins and, predictably, led to the first banking fraud. Johan Palmstruch, general manager of Stockholms Banco, used his privileged position to issue more notes than his bank had the silver deposits to redeem and in 1668 he was prosecuted for fraud.

Adulteration

During the late 18th and early 19th century, with industrialisation taking hold around the world, the availability of natural resources became ever more acute. This amplified an already-established type of fraud – food substitution. While food stuffs had been adulterated since the early days of trading – with high value spices, for example, mixed with ground nutshells or dust – this period witnessed a significant growth in the practice. Milk was frequently diluted with dirty water or bulked up with chalk; sawdust was added to flour to reduce the amount needed to bake each loaf. The scale of the problem can been seen in the introduction of food laws across the globe, although it was not until 1860 that the UK passed its first Food Adulteration Act. Food fraud, of course, continues to this day, with the horse meat scandal of 2013 being the latest high profile example.

below: **Telegraph, Morse apparatus, Trousset encyclopedia (1886 - 1891)**

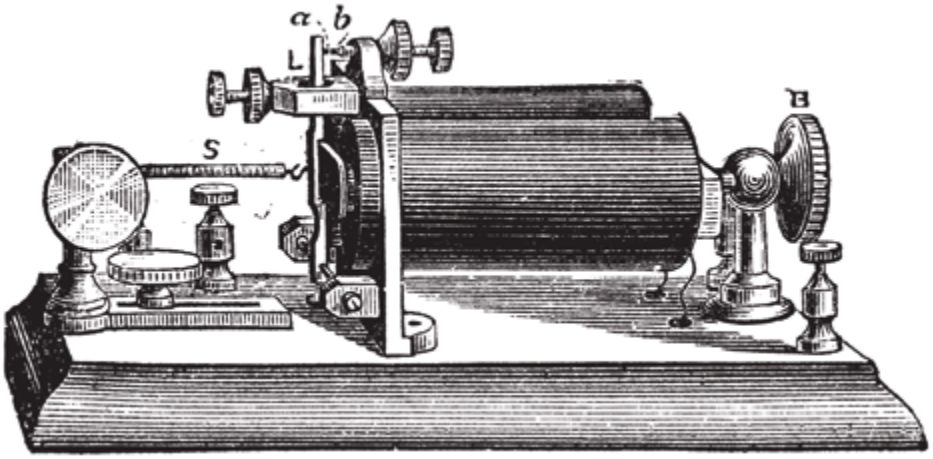
above: **Paper Currency of Ming Dynasty (1368-1399), Magasin Pittoresque (1882)**

The telegraph

Industrialisation in the 19th century also resulted in increased fraud because trade now required speedy communications. In 1867 a Wall Street stockbroker collaborated with Western Union telegraph operators in an attempt to move the stock price by intercepting dispatches sent to eastern US newspapers and substituting fake messages suggesting the imminent bankruptcy of certain companies. The century also saw a rise in both the availability and use of credit for business transactions. The growing popularity of credit brought the rise of the debtors' prison but also the emergence of the 'long firm fraud', which made it into the *Oxford English Dictionary* in 1882: 'that class of swindlers who obtain goods by pretending to be in business at a certain place and ordering goods to be sent to them, generally from persons at a distance, without any intention of payment'.

'Education has to be the way forward. As cybercrime attempts increase, law enforcement will struggle to prevent or investigate every incident because of the international nature of the crime. Education can have an international impact, but crucial to its success is reaching people from an early age with a consistent message.'

Tony Neate, chief executive, GetSafeOnline



Old Ponzi

The 20th century, with its ready access to financial markets and expansion of personal investing, saw a huge increase in fraud. Perhaps the most well-known was that of the American Charles Ponzi in the 1920s. Ponzi duped investors by exaggerating the margin on the purchase and sale of discounted postal coupons. Investors jumped at the promise of 50% returns, not realising that Ponzi was paying dividends to early investors with the new money committed by the recent ones. By the time the fraud was finally discovered Ponzi had made $10m and fled the country.

After the Great Depression the 1940s saw many countries introduce comprehensive welfare systems and fraudsters were quick to exploit any obvious weaknesses. In the US the system of food stamps, brought in during 1939, lasted only six months before suffering its first confirmed fraud. And in the UK social security fraud rose steadily through the rest of the century.

Charles Ponzi was arrested on 12 August 1920, and charged with 86 counts of mail fraud

The telephone

In the 1960s the popularity of household telephones, primarily in the US, provided an opening for telemarketing scams, the predecessor of the modern 'boiler room' frauds in which low value shares are 'pumped and dumped'. Relatively high call costs also led to a phenomenon known as 'phreaking' in which householders reverse-engineered the tones used to route long-distance calls, allowing them to call toll free. Some notable proponents of phreaking were Apple founders Steve Jobs and Steve Wozniak.

'Modern discussions of fraud largely ignore the historical perspective. From the comments of most police, politicians and media, we might assume, for example, that transnational fraud is a purely contemporary phenomena. But whilst the internet has undoubtedly had a significant effect on the cheapness, ease, scale and reach of fraud, its impact has proved to be no more influential than developments such as shipping, rail and the invention of the telegraph. And whilst technologies have democratised opportunities to commit fraud, many contemporary scams still rely, as they have always done, on privileged access – be this to power, pools of wealth, or wealthy victims.'

Michael Levi, professor of criminology, Cardiff University

1980 Denial of service / extortion / sabotage
1980
1985 Funds transfer fraud / ATM fraud
1986 Espionage
1990 Child exploitation
1993 Botnets
1995 Online piracy / identity crime / spam
1997 Cyber terrorism
1998 Cyber stalking

New Ponzi

The 1970s saw the creation by New York stockbroker Bernie Madoff of what is still regarded as history's highest value fraud. His company, Bernard L. Madoff Investment Securities LLC, was a gargantuan Ponzi scheme that purported to invest in standard financial products. It was exposed in 2008, during the global financial crisis, by which time it had taken $64.8bn in deposits.

The 1980s were characterised by large-scale corporate frauds around the world. In the UK this was typified by the Guinness share trading scandal. Along with other high profile cases this led to the introduction of targeted legislation and the creation of new enforcement bodies including the Serious Fraud Office (SFO).

The internet

The 1990s saw the introduction of a technology that has arguably made the greatest impact on the volume of fraud committed during the 20th century and beyond – the internet. Formed as the 'world-wide web' in 1991, the internet has proved a very efficient platform for communication and commerce. Furthermore, it has enabled traditional frauds, such as the Nigerian 419 investment scams, to migrate from letters to mass-marketed emails. And that is the world into which the Fraud Advisory Panel was born in 1998.

2000 | 2002 Phishing | 2003 Wireless vulnerabilities | 2006 m-commerce attacks | 2009 Cloud computer attacks | 2013 RFID card attacks | 2014 Biometric compromise | 2015 Internet of Things attacks | 2017 e-Voting attacks | 2018 Virtual currency attacks | 2020

The changing face of modern fraud

In the late 1990s both the experience of fraud and the response was mostly local, low-key and low-tech.

After a decade of big corporate scandals – Guinness (1987), Polly Peck (1991), Maxwell (1992), BCCI (1993 and 1995) – many people thought fraud was solely a management crime, to be tackled by the SFO (with varying degrees of success). Otherwise, it was 'victimless', with the actual victims getting little or no sympathy or support. Companies, it was said, could afford it; individuals must have been greedy or stupid.

A paper-based criminal justice system struggled with complex cases and could easily be overwhelmed by technical evidence. Documents stored on a computer had to be accompanied by proof that the machine wasn't faulty. Many fraud prosecutions had to be conducted under the 1978 Theft Act, making them prone to mishap. The Law Commission was not in favour of a simple new offence of fraud.

No-one in government was charged with promoting a measured, comprehensive and consistent response, so 16 departments and agencies all had some fraud-fighting duties. Nor was fraud a national policing priority. Research into the true nature, extent and impact of fraud was very much in its infancy, and politicians lacked the appetite and will to acknowledge and deal with the reality.

Cybercrime shows its true colours …

By 1999 signs of a coming cybercrime crisis were easy to find. Bogus websites were already harvesting credit card details and hackers stole confidential information, often using tools found easily online. British business was wide open to this threat. Four-fifths of companies using 'electronic links' had no firewall. Poor password security was rife.

The Melissa virus (the worst to date, March 1999) infected a million computers worldwide and did damage worth £50m. Just 14 months later the Love Bug struck, infecting 45m machines and crippling even the Pentagon's email system. Putting things right cost more than $8bn. Its payload of malware was disguised as a love letter, introducing the world to 'social engineering'.

Identity theft caused losses of more than £1.7bn in 2006 (Home Office estimate). Then they trebled, to £5.4bn, over the next 10 years.

The number of identity theft cases reported by Cifas members doubled to 174,523 in the decade to 2017.

The 113 unique phishing attacks registered in December 2003 (the month the Anti-Phishing Working Group began collecting data) grew to 98,072 by September 2017, along with 57,317 new phishing websites detected.

… and settles in for the long haul

January 2007 saw some watershed developments in the fight on fraud and cybercrime. The Fraud Act 2006 and the first iPhone entered the world almost simultaneously. At about the same time domestic access to broadband began spreading rapidly, reaching half of UK households in 2009. Arguably, fraud fighting has been on the back foot ever since.

Fraudsters look for three things: the chance to remain undetected; speed in committing the crime; and naive or unwary victims. The modern internet age handed them all three, on a plate.

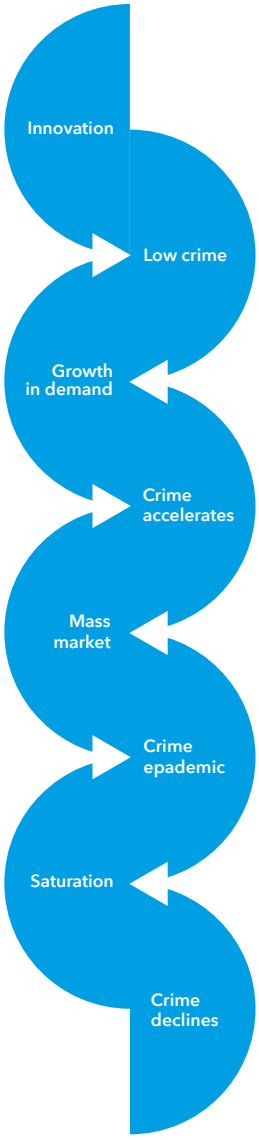
Opportunity theory (see diagram 1) puts it another way: predatory crime rises when 'motivated offenders' have more 'suitable targets' and there are no 'capable guardians' to stop them.[1] And so it was, and is. Not much can be done about the motivations of a generation of fraudsters. But sweeping social, technical and economic transformation was always going to change the criminal calculus, especially if our defences systematically underestimated the threat.

Business

Criminals were given exactly the tools they needed to commit increasingly sophisticated and damaging acts with impunity, with no compensating mechanisms sufficient to keep the rest of us safe. The wider world invested heavily to transform every aspect of our daily lives but, again, with little thought for the crime and security consequences.

Excessive demands for personal information by mainstream businesses have long softened us up, shoppers and investors alike, for the fraudster's call or email. Vast, poorly protected corporate databases are a magnet for criminals and frequently breached.

Diagram 1. **The consumer technology lifecycle creates new criminal opportunities**



'Blockchain *is* the fraud, in most cases. An intellectually interesting technology with few actual real-world uses, that's been hijacked by charlatans as a jargon-word magic-spell to relieve the desperate of their money.'

Ben Hammersley, journalist, futurist and technologist

Banks remain complacent about service innovations that often make customers more vulnerable. People tricked into sending money to a criminal's bank account lost £236m in 2017, of which only £60.8m (26%) was returned to them by their banks.

Two-thirds of fraud losses from unauthorised use of payment cards, online banking and cheques were averted by bank systems in 2017. The remaining third still represents a loss of £731.8m to customers.

Many traditional banks rely on legacy systems that struggle to cope with the demands of modern internet-enabled finance. At the start of the year new, 'open banking' rules (to increase the sharing of customer banking data with third parties) were introduced in a rush in spite of customer confusion, concern and reluctance. This new regime will put further immense strain on creaking bank systems and, inevitably, expose customers to new threats from hackers and bogus providers.

Peer-to-peer lending and crowdfunding – both being online services to match lenders with borrowers directly – have also created new opportunities for benefit and harm.

Last year a British Banking Association (BBA) study found that almost all banks surveyed (92%) feared that within two years their legacy systems would become an obstacle to fighting crime.

Recent data abuse scandals, sweeping social media providers and political campaigning, are exposing business models not unlike identity frauds; personal data harvested, exploited and traded without permission then used to peddle deceptions (such as fake news) for advantage.

Government

Government began moving its services online in 2011, when a quarter of households still had no connection. Why then was it so slow waking up first to fraud and then to cybercrime? Since 2010 austerity economic thinking has had predictable consequences for the criminal justice system. Today the vast majority of fraud is still not investigated and an already-low risk of prosecution has become vanishingly small.

'Blockchain is a technology that promises greater security and trust. But, like any new technology, fraudsters will attempt to leverage the public's enthusiasm and limited knowledge of the new platform. Once the technology becomes mature it could help enhance information and trustworthiness, but people should be careful while the hype is still high.'

David Lyford-Smith, technical manager - IT and the profession, ICAEW

A long-trumpeted 'failure to prevent economic crime' offence remains bogged down in cabinet a year after the consultation ended. An effectively unregulated and widely abused company registration scheme, easily accessible online since 2011 for a £12 charge, remains a gaping hole in our criminal defences and our international reputation.

Rapid increases in the price of bitcoin have triggered widespread concern about a new investment bubble, but also revealed that cryptocurrencies are still, in spite of their immense popularity among criminals, largely unregulated.

Now Brexit is spreading uncertainty, confusion and cynicism that are a gift to the fraudster. New systems and processes, almost certain to be introduced in a hurry, will create new fraud vulnerabilities, just as the creation of the European single market did in 1993 with carousel VAT fraud (UK losses of £20-30bn over 10 years).

Law enforcement

The City of London Police has steadily upped its game since becoming the national lead force. The National Crime Agency (founded in 2013) has a genuine counter-fraud capacity in its economic crime command. But a police officer quoted in the most recent Cifas Fraudscape talks of 'chasing Formula 1 cars on a tricycle'. The weak police response to today's high street 'fraud boys' (who use social media to recruit young money mules, and whose identities are often well-known locally) suggests another problem. Our 2016 study of the Fraud Review's legacy found many local forces neglecting fraud reports even when a rapid local response could prevent losses, then using the existence of Action Fraud as their excuse.

Tweet tweet

Replacing so many of our face-to-face contacts with anonymous, opaque and ambiguous interactions over the internet has short-circuited millennia of social evolution.

Social media that made it cool to share every last thing also makes it child's play to research and locate the most promising victims and then design the perfect con.

Today's 'Nigerian letter' (or 419) frauds are carefully-crafted, personalised and electronic – and supported by expertly forged documents, websites and social media profiles.

Investment fraudsters no longer simply mislead, they actively 'groom' their victims, research their lives, circumstances and social support networks online, then customise the crime to maximise and exploit the weaknesses.

In 2017 Equifax found: 55% of people still willing to use public Wi-Fi without password protection; 40% with no antivirus software installed; 27% using the same password repeatedly; and 32% who knew they were putting themselves at risk.

The fetish for super-fast everything, operating at the limit of our instincts, leaves little time to be smart or circumspect, or even to simply double-check a URL or email address.

And many internet users are still very far from competent. In 2016, 5m adults lacked basic reading, writing and numeracy skills. Many more – 12.6m – struggled with email and online forms because they lacked basic digital skills.

Meanwhile, savvy young people in the tech, gaming and coding communities are being drawn to the dark side by a different kind of deficit – they don't understand the true damage they do and are unaware of the legal opportunities for young people with cyber skills and talent.

What next?

The explosion of fraud and cybercrime is not an act of nature. Nor did it appear without warning. It represents a comprehensive failure of imagination by industry, law enforcement and government. A failure which allowed new technology to rapidly increase the exposure of honest citizens to predatory crime while simultaneously hobbling their guardians.

The chair of the government's Secure by Default expert advisory group warns that current password security advice is impractical for a household with hundreds of networked devices. There is a growing expert consensus that market forces and consumer education are not enough to make the coming internet of things (IoT) secure.

Instead strong security needs to be designed-in from the very start. But, as usual, the security debate began only after the first devices were in the shops, by which time it was already too late.

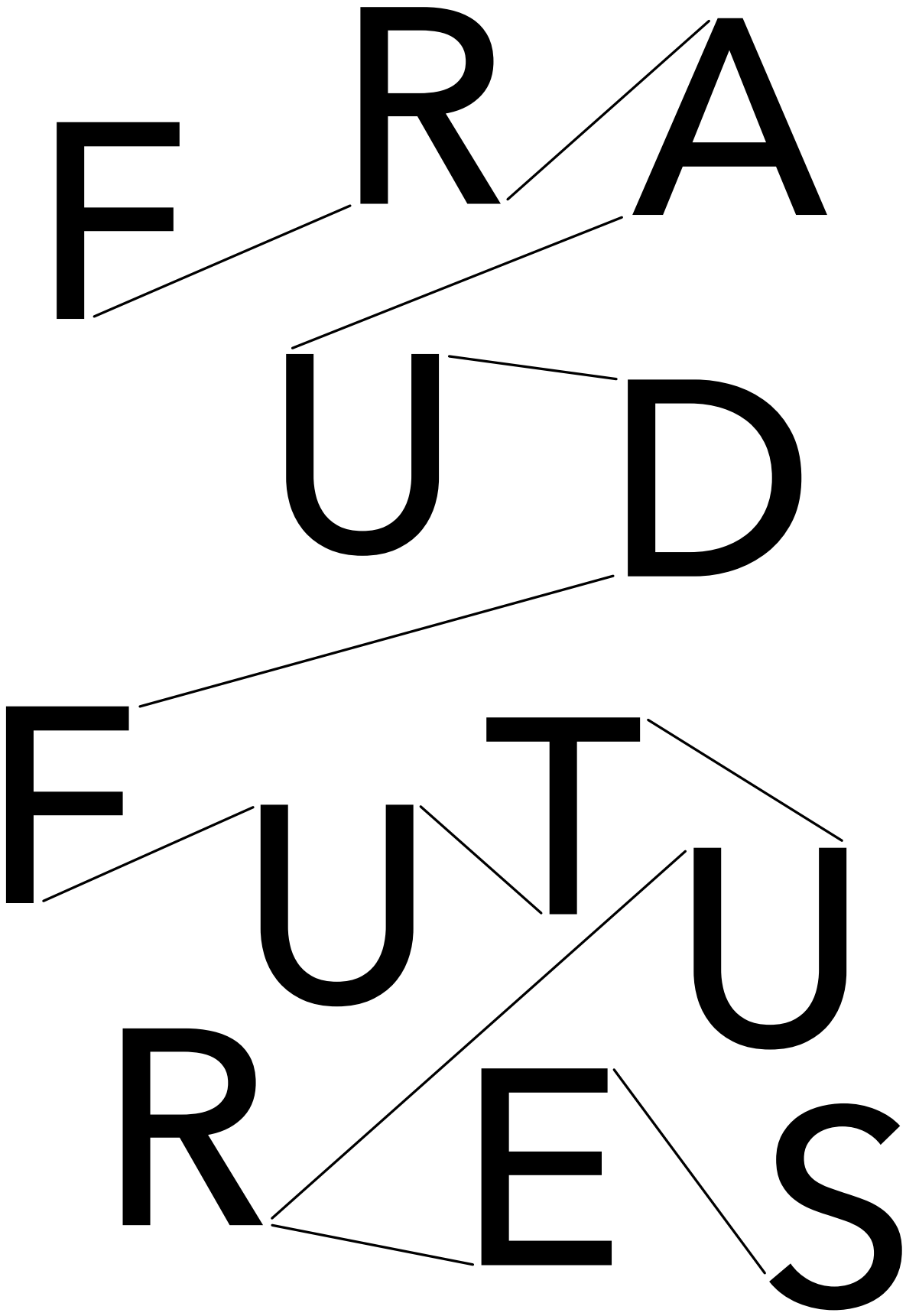
A new DCMS report – *Secure by Design: Improving the cyber security of consumer Internet of Things* – says that the government still prefers a market solution based on voluntary compliance by product developers.

Meanwhile, public hearings about data harvesting and social media prompted concerns that too many senior lawmakers have too rudimentary an understanding of the technology and its consequences to be effective regulators.

This is not good enough now but even bigger challenges lie ahead.

The criminologist David Wall talks about three generations of cybercrime. The first was unwieldy mainframe computers facilitating traditional crimes. The second saw the hacking of computer networks. The third is upon us today: attacks that are fully automated, distributed and mediated by technology, as when botnets distribute spam.

We know that the IoT will increase the present threats manifold. But, as our futurologists reveal on the pages that follow, a fourth generation of cybercrime is arriving fast.



We asked six leading thinkers to each consider the future fraud threats emerging from new developments in their own specialist field. The picture they collectively paint is a chilling one.

Artificial intelligence

Kevin Warwick, emeritus professor, Coventry University

Artificial intelligence (AI) and robot technologies are already having a dramatic effect on society in many ways. In the next decade they will have a profound impact in the area of fraud – both in detecting and facilitating it.

AI is good at classifying data into groups and predicting likely outcomes. It is also able to deal with multi-dimensional information, while the human brain has problems with anything above 3D. So AI is very useful where lots of different types of information are available. This has already been put to good effect to analyse shopping habits, particularly in supermarkets, by linking different products with shopper types.

Something similar can be applied to fraud prevention and detection. Any AI system will only be as good as the accuracy of the data that it operates on, so the validity, quality and provenance of the data will be an important issue in fraud applications. And the more data that is available (so-called big data), the better the fraud analysis job that can be done.

Over the next 10 to 20 years we will see dramatic changes both in the number of AI systems taking over a controlling role and the nature of their interface with the human brain. One obvious example is the dramatic impact that autonomous vehicles will have on our transport system, with no future need for such things as traffic lights, road signs and lane markings.

Even now AI is starting to change how we understand our own brain. Using electrodes AI can predict the onset of Parkinson's disease by modelling parts of the brain, and even help surgeons in their understanding of the exact problem. But electrodes are often not necessary. For example, biometric analysis can be used to give an indication from typing habits of who is entering information via a keyboard. At present this technique may not be able to say exactly who you are, but it can say who you are not! Clearly its performance will improve in the years ahead.

The human brain uses something called 'deep learning' in that we can witness what a person does but it is not possible to infer behaviour from looking at individual brain cells. Latest AI systems, based on neural networks, are constructed in the same way. We will have to get used to accepting what the AI tells us, without worrying about how it comes to its conclusions.

But it is in communication that we will see the biggest impact of AI, as we start to communicate more directly between brains. Speech is clearly antiquated. Exchanging thoughts would allow signals to remain in electronic format as they pass between brains. Although a portent of a much more intimate future – which will be what people want – it will also open up new opportunities for hacking. You may want to simply think to someone else, but will you be sure of their identity, and who else might be reading your thoughts?

Blockchain

Kevin Curran, professor of cyber security, Ulster University

Blockchain has become an important technology in a relatively short time, with major implications for the future security of our systems.

Bitcoin is arguably the most famous blockchain system. Its popularity is due in no small way to the ingenuity of its underlying framework. A publicly accessible ledger of all confirmed transactions (plus any added through the bitcoin mining process) prevents the dreaded 'double spend' which afflicted many previous attempts to create a usable virtual currency. What is clever, however, is that it can be difficult to associate any one address in the network with any other, so people can remain anonymous provided they use different bitcoin addresses and 'mixing' technology (anonymised coin swapping).

This separation of virtual currency accounts from real-world identities, along with the ability for an individual to create an arbitrary number of accounts, also enables users to develop novel, complex layering transaction patterns. Newer cryptographic anonymity solutions, such as Zerocoin and Zerocash, have incorporated stronger, protocol-level mixing to provide true anonymity and cryptographic guarantees. (Bitcoin is also working on strengthening anonymity.)

By providing almost perfect anonymity, bitcoin has enabled hackers to demand ransoms in the knowledge that the payments will probably be untraceable. This has already led to a rise in ransomware attacks and we can expect to see this type of cybercrime continue to develop as a highly lucrative and well-organised enterprise.

We may see 'smart' home devices held hostage and owners expected to pay a fee to recover the use of their lights, their heating, or some other internet of things (IoT) appliance. We may also see ransomware appearing on our smart cars, trucks, trains and planes. It is only a matter of time before we see people left helpless by the side of the road, unable to drive their vehicles until they pay a ransom. Blockchain-based cryptocurrencies like bitcoin will have critically enabled all of these crimes.

This is a pivotal moment in global society where financial transactions can take place without being traceable. We are starting to see virtual currencies forming part of the modus operandi of trade in illicit goods – such as weapons, drugs, child abuse material – as well as regulated services like online gambling. It is time to examine the implications for society of such a powerful, anonymous tool.

Blockchain-based cryptocurrencies are here to stay. However, for the foreseeable future law enforcement and regulators are facing a crisis in their ability to investigate these virtual transactions. The skills required to 'follow the money' have exploded overnight. In future, we are likely to need dramatically more and better trained computer security incident response teams, supported by real-time collection of traffic data as well as stronger search, seizure and expedited preservation powers over stored computer transactions.

What is blockchain?

Blockchain is a distributed database that maintains an ever-growing list of data records secure from tampering or revision. It is de-centralised to avoid a single point of failure. Users work together to confirm the legitimate new transactions. So a blockchain is composed of time-stamped data structure blocks, with each block holding batches of individual transactions (plus the results of any blockchain calculations) and being linked to the previous block. The blockchain therefore serves as a public ledger of transactions which cannot be reversed without great difficulty. The technology has the power to transform key aspects of society for the better. For example, smart contracts based on blockchain can make micropayments more cost effective. In the music industry it could enable data sharing among the value chain, from artist to final consumer, helping to realise and release more value, to track who owns and contributed to a creative work (eg, a song), and to enforce an unambiguous ownership trail.

Cybersecurity

Dr Ian Pearson, futurologist, Futurizon

As a technology futurist, it seems clear to me that security will become much harder in the future and there will be greater opportunities for fraudsters. Here are just a few examples.

Miniaturisation already allows a computer with hundreds of thousands of transistors to be made smaller than a millimetre across. In a decade that could be 0.1mm, the threshold of normal human vision. 'Smart dust' will be just that. If your keyboard is like mine there are millions of dust particles on it, any of which could be 'smart', listening to my phone calls or deducing what I am typing from the sound and direction of the clicks. Others could be inside my PC, sitting on wires and monitoring the signals travelling through them. Other than inside a cleanroom, it will be near impossible to exclude such tiny devices.

A fraudster could contaminate your clothes with smart dust simply by brushing against you. Or a mist of particles could emerge from a briefcase or handbag to contaminate many people at once, all of whom would then become sources of occasionally sensitive data. Even a handshake could contaminate you with smart bacteria (next generation smart dust). The fingerprint sensors and keypads of shop payment devices or cash machines could easily be contaminated so that PINs and fingerprints can be stolen and face recognition via hidden cameras used to identify the people they belong to.

Artificial intelligence (AI) is a source of risk as well as a major help in detecting fraud. For example, AI can recognise facial expressions and lip-read better than most humans, increasing the ease with which sensitive data can be captured using far away hidden cameras. Worse still, AI can now reproduce your voice fairly convincingly after just a few seconds of exposure. If a fraudster has managed to get access to your data, they could pretend to be you much more easily. Reproducing your mannerisms, gestures, signature and voice, while probably knowing your PIN or passwords too, will all become feasible. New types of display will even allow iris scanners to be misled.

Biometric theft is a bigger problem than many imagine. Every time you stay in a hotel room, or use a train seat, you leave behind flakes of skin or hairs. There will be a DNA black market, with the price increasing if the sample is accompanied by fingerprints from a glass or tap and identity information from occupancy records or scraps of paper left in a bin. Even if the thief can't use the DNA samples themselves to steal from you, they may be able to sell them on to someone looking to plant incriminating evidence at a crime scene.

Passwords are becoming less useful, and we've already seen how the desire for convenience, such as keyless entry, has led to car thefts. This shows how much security is routinely overlooked or poorly understood. As IoT devices multiply there will be many more examples of this. Bad news for security, but lucrative opportunities for the security industry.

Data - the big steal

Dr Simon Moores, managing director, Zentelligence (Research) Ltd and former government technology ambassador

'I'm not here to predict the future' quipped the novelist Ray Bradbury, 'I'm here to prevent it.' And the future looks much like one where giant corporations who hold the most data, the fastest servers, and the greatest processing power will drive all economic growth into the second half of the century.

We live in unprecedented times. Nobody knows what the world will look like in 20 years. Making confident forecasts in the face of new technologies has become a real challenge. The few real certainties available to us concern the uninterrupted march of Moore's Law – that's the notion that computing power (more specifically the number of transistors in a top-of-the-line processor) doubles approximately every two years – and the unpredictability of human nature.

Experience tells us that where new opportunities for fraud and financial crime exist, the 'dark market' will expand to meet them. Asked why he robbed banks, the gangster John Dillinger replied: 'Because that's where the money is'. Today is no different, other than a growing appetite for stealing data, offering potentially higher and safer returns to criminals than robbing banks.

Over the last 12 months we have seen just such an alarming and growing development, one which we have every reason to believe will continue to grow. Sophisticated criminal gangs, perhaps even nation states, have been exfiltrating and harvesting ever larger volumes of seemingly innocuous data from businesses and government departments across the planet. In October 2016 hackers stole the personal data of 57m customers and drivers from Uber. By far the biggest breach so far was the theft of India's one billion-strong public database of personal details earlier this year. It is clear that even relatively innocuous personal information, such as our browser search history, is worth a vast amount of money when taken in aggregate.

The question that vexes many observers of an increasingly dystopic information security space is why? In March 2017 I remarked in *The Guardian* newspaper: 'A rapid convergence in the data mining, algorithmic and granular analytics capabilities of companies like Cambridge Analytica and Facebook is creating powerful, unregulated and opaque ''intelligence platforms''.' However, these two influential and powerful companies are simply those whose interests and activities most visibly coincide in repurposing consumer data, aggregating and analysing it for profit.

There are likely to be many other unknown operations, working away in the shadows, sharing, analysing and exploiting the huge volumes of data regularly stolen, and doing so for a whole spectrum of often-criminal purposes.

There are three convergent trends here, which projected-out to the near future we should be wary of: machine learning and artificial intelligence; rapid advances in quantum computing; new and cost-efficient cloud-hosted services for big data aggregation and advanced predictive analytics. Together they add up to advanced computing capabilities more commonly associated with western intelligence agencies.

The scandal surrounding Cambridge Analytica and Facebook has arrived as a sharp wake-up call about the growing importance of personal data. It's entirely possible that well-funded, well-organised and forward-looking criminals are simply stock-piling the terabytes of encrypted information they steal, awaiting the breakthroughs (perhaps within the next five years) in cloud-hosted quantum computing, cryptography-breaking algorithms and analytics for rent that will unlock it all for them.

By 2020 there will be some 50bn connected devices as the internet of things (IoT) continues to expand near exponentially. Every minor detail of our lives will silently deliver a stream of tracking and personal telemetry and data points. More than 44Zb (1 zettabyte = 1 trillion Gb) of data in total by 2020, growing at a rate of 1.7Mb per person per second. In isolation much of it would be worth nothing. In volume, aggregated and analysed at scale, it will be of enormous value – a treasure trove to anyone planning a finely-crafted identity theft scheme, just one among many criminal possibilities.

'Data is the new oil' wrote *The Economist* magazine in 2017. An exaggeration? Perhaps. But for organised criminals, with a growing arsenal of cheap and powerful data mining and hacking tools at their disposal, data is most certainly where the money now is. If you haven't lost yours to a passing hacker yet, then you are very likely due a visit sometime soon.

The digital workplace: freedom or distraction?

Dr Nicola Millard, head of customer insight and futures, BT

'Digital' work means many things to many people. To some it's all about the technology, but digital runs deeper than that. You can't just *do* digital; you have to *be* digital. And that requires a change in culture, collaboration, transparency and trust.

Digital work is enabled by technology. That technology is shrinking in front of our eyes. What used to require a desk to put it on now fits inside a small shoulder bag. We have become untethered from our physical offices, while simultaneously being constantly connected to them digitally.

We value the freedom this gives us. In our recent global employee survey, 76% said that the ability to work flexibly was their top choice of employee benefits package (over traditional perks like a company car).

But this flexibility can come with some challenges.

'The problem of the future won't be connection, it will be disconnection', predicted *Wired's* Kevin Kelly. When we can work anytime, anyplace and anywhere, should we be expected to be 'always on'? If we are never in the office, how do we manage people we never see? If productivity is now defined by our availability on instant messenger rather than our visibility in the office, is there pressure to never disconnect?

Connection is vital to collaboration. But constant connection can decrease the productivity gains we get from the flexibility of the digital workplace.

Because of the number of demands on us during our work day, we are multitasking – effectively juggling a series of single tasks. The issue with this is that we become wired for distraction.

Task-switching – caused by interruptions, both physical and from the devices that are always on and always on us – can seriously impact productivity. It can take us between 12 and 20 minutes to get back into the pre-interruption train of thought.

We tend to compensate for this inefficiency by working longer hours, and the downward spiral of productivity dips further as we get tired. Switching off occasionally (our minds too, not just our technology) can have huge productivity benefits, not least because it puts us in control.

Control is essential – classic psychology tells us that a job with high demand and low control will result in stress.

This is especially relevant in an age of artificial intelligence. AI is good at boring, repetitive and mundane tasks. This leaves us with the tasks which are, by definition, inefficient and messy precisely because they cannot easily be quantified and automated. These are generally tasks which best engage the human brain, but they are also those which are most likely to require deep concentration and extensive collaboration.

The leadership challenge is to rethink productivity for a digital age.

Collaboration among virtual teams doesn't happen by magic, it happens by purpose. This includes putting in technologies which allow people to connect wherever they happen to be. But they also need to ensure that work, technologies and spaces are designed to make it as easy to disconnect as to connect.

The evolution of fraud

David Canter, emeritus professor, University of Liverpool and visiting professor, Liverpool Hope University

Fraud has always been with us. Even the opening chapters of the Old Testament have a couple of examples. Like all human activity it can be regarded as an organism that evolves to take advantage of new habitats as they emerge.

Some of these evolving fraudsters just adapt their existing tactics to the new situations. In some situations entirely new types of fraudster emerge to take advantage of radically new opportunities, whether that is new laws (such as the tariff systems that will be in place after Brexit) or new ways of gaining access to other people's money. But the old possibilities never quite disappear, allowing existing villainy to carry on as before.

When thinking of the sorts of fraudsters who are likely to be active in the middle of the 21st century it is important to note that they are currently in primary school or in their teens. They are growing up in the explosion of social media and interactions over small screens, using high level computer software. Even a high-tech culture in which a sucker is never given an even chance will still generate relatively unsophisticated opportunist fraudsters. They will see a gap in security, or will learn about it through social media, and take advantage of it. These people will be the same sort who years ago, before banks checked identities more carefully, sent couriers to cash forged cheques or set up fake bank accounts.

Other, more skilful fraudsters, those who currently are aware of the details of banking systems and can use social engineering to gain access and squirrel away funds, may find life more difficult if the banks do eventually get their acts together and start identifying and closing suspicious accounts instantly (the days and weeks it currently takes is unconscionable). But, just as increased motor vehicle security caused more aggressive forms of theft to emerge, such as car-jacking, so we may see people once more forced to transfer money at gun-point, like highway robbery in the age of the stage coach. More subtle exploitation of vulnerable victims – by developing insincere relationships or even blackmail – will doubtless continue as today.

The expert (some might even call them 'professional') fraudster – capable of creating systems to access other people's money – could emerge as a new breed. Steeped in computer code, enjoying the challenge of breaking into online security systems, these people might once have been the stereotypical lone-teenager-in-their-bedroom. With the increasing complexity of what is casually called 'the internet', lone teenagers are increasingly likely to give way to organised networks; a futuristic version of Dickens's Fagin and his gang of pickpockets.

So, in 10 or 20 years' time, many fraudsters will not look so very different from those active today – some will even be the same people, but with their skills honed by increasing success. There will be the angry employees who believe they deserve what they take; the business men and women who think fraud is a noble act if it saves their company; and the people brought up in a criminal culture for whom access to other people's wealth is a lifestyle. But also some fresh new players, who will regard the excitement of beating 'the system' as simply a form of entrepreneurship, a natural consequence of the novel opportunities they become aware of.

Search ‘artificial intelligence and fraud’ and you will find plenty of advice on how this exciting new technology will soon help us right wrongs of all kinds, including fraud. The same is true for ‘big data’ and ‘blockchain’.

But a recent report by the international Future of Humanity Institute[2] reminds us that new technologies like AI and robotics will also free the fraudster (and the organised criminal and the terrorist) from their human limitations.

These are unimaginably powerful tools. Their misuse will make life very miserable for some, possibly for many.

Voluntary codes of conduct, updated password advice and market-led solutions have served us poorly in fighting the present incarnation of cybercrime. They won’t be anything like enough to stop the next one either.

Fraud fighters of today and tomorrow must learn from the past if we are to anticipate the future.

Acknowledgement

The Panel would like to extend its warmest thanks to everyone who contributed to the writing of this report, in particular: David Canter, Kevin Curran, Nicola Millard, Simon Moores, Ian Pearson and Kevin Warwick *(Fraud futures)*; Oliver Shaw *(A brief history of fraud)*; and Trevor Maggs *(The changing face of modern fraud)*.

End notes

[1] Smith, RG, 2010. The Development of Cybercrime: An Opportunity *Theory Approach in Lincoln, R and Robinson, S (eds). Crime over time: temporal perspectives on crime and punishment in Australia.* Cambridge Scholars Publishing (pp 211 – 236).

[2] University of Cambridge Centre for the Study of Existential Risk, 2018. *The malicious use of artificial intelligence: forecasting, prevention and mitigation* [pdf] 21 February.

FRAUD FUTURES

‘In the future there will be a tailored local response to fraud which will include a direct focus on fraud victims. There will be wider recognition not just of the scale of fraud but a much deeper understanding of the impact it can have, which in some cases is every bit as serious as a physical attack.

We will need to look beyond the police though and, indeed, beyond the range of current providers where fraud victims’ needs are rarely understood or prioritised.’

Professor Martin Gill, director,
Perpetuity Research & Consultancy International (PRCI) Ltd

FRAUD ADVISORY PANEL

Chartered Accountants’ Hall,
Moorgate Place, London EC2R 6EA, UK
T +44 (0)20 7920 8721
E info@fraudadvisorypanel.org
www.fraudadvisorypanel.org

Company Limited by Guarantee
Registered in England and Wales
No. 04327390
Charity Registered in England
and Wales No. 1108863