ACCA Think Ahead

EY Building a better working world

Economic crime in a digital age

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants, offering business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management.

ACCA supports its **219,000** members and **527,000** students (including affiliates) in **179** countries, helping them to develop successful careers in accounting and business, with the skills required by employers. ACCA works through a network of **110** offices and centres and **7,571** Approved Employers worldwide, and **328** approved learning providers who provide high standards of learning and development.

Through its public interest remit, ACCA promotes appropriate regulation of accounting and conducts relevant research to ensure accountancy continues to grow in reputation and influence.

ACCA has introduced major innovations to its flagship qualification to ensure its members and future members continue to be the most valued, up to date and sought-after accountancy professionals globally.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability.

More information is here: www.accaglobal.com

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over.

We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy.

For more information about our organization, please visit: ey.com

January 2020

Economic crime in a digital age

About this report

Economic growth flourishes on technological advances, and the current rate and impact of change is unprecedented. But criminal activity also responds and reacts, and the opportunity that criminals exploit creates challenges for regulators, legitimate businesses and their customers, auditors and advisers alike. This report draws on recent thinking from senior leaders across EY and ACCA's networks to reflect on the current position and highlight some key pointers for the way ahead.

Foreword

Up to $3.5 trillion per year – that's how much financial crime costs the world. That's more than the GDP of the UK. And financial crime takes a human toll. People suffer. They lose savings, jobs and sometimes much more.

Evaluating the role of technology in financial crime is an important piece of the puzzle. It is an elusive and rapidly evolving issue. Criminals are not going to wait for us to catch up.

New technologies have increased the speed of individual financial crimes. Phishing, for example, can happen with the click of a button. Financial crimes are not just faster, but they are more numerous than ever and technology has become a vector for novel criminal activity. It is important to identify why those crimes have arisen. The answer lies in the positive relationship between technological advances and value creation. Organisations are making money in new ways. Criminals have responded creatively.

It all comes back to trust. As this report makes clear, every financial crime is an abuse of trust. This is where professional accountants can make their mark. Technology cuts both ways: it is a vector for crime, but it is also a tool for creating tremendous value and protecting it from financial criminals. But tools alone are not enough to fight crime. People will make the difference, and professional accountants, as widely trusted actors, are at the centre of the action in every organisation.

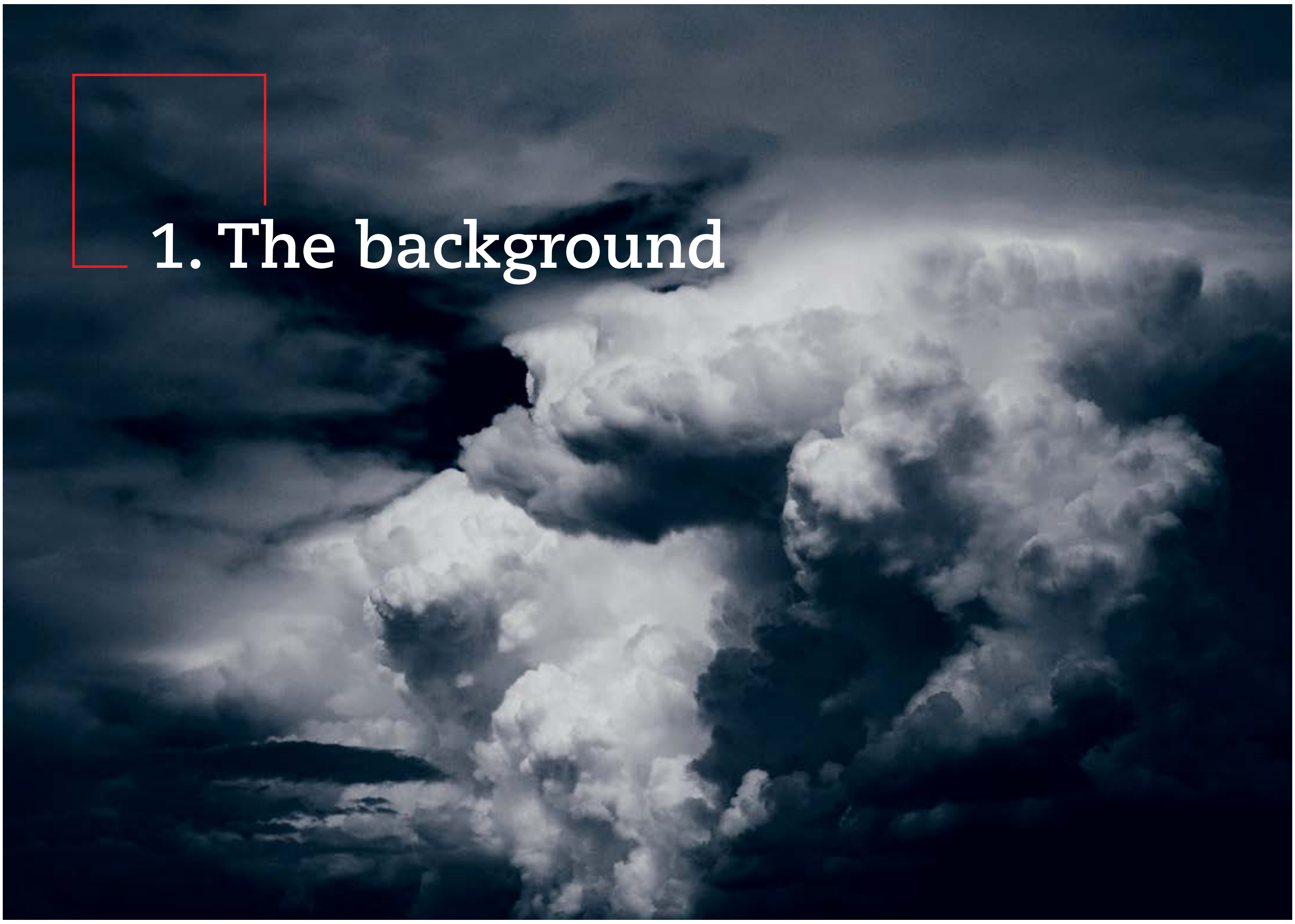
The profession has always stood out for its independence and scepticism. Our challenge is to adapt – and keep adapting – to a continuously changing economic and technological environment. We are up to the challenge, and we embrace it.

We can act. Technology will empower professional accountants to add more value and add it in new ways. They can make a strong case that 'know your client' (KYC) checks are not just a compliance function. And professional accountants can, and should, stake out realistic expectations for their roles, and advocate agile standard-setting that keeps pace with change. The profession is at the heart of this fight as no one else is, in both the private and public sectors.

Professional accountants are at the centre of human responses to financial crime, through their professional work and public voice. Political borders are less relevant than ever to criminal activity. A piecemeal response won't cut it. The world needs global action and cooperation. This report serves as a compelling call to action for the accountancy profession to lead the way in fighting financial crime.

Kevin Dancey
CEO, International Federation of Accountants (IFAC)

Contents



1. The background

Society relies on the creation and exchange of value and the reallocation of surplus production to build and sustain everything, from physical infrastructure to works of art. But the mechanisms developed over the centuries for measuring and assigning that value are under constant attack.

Trust, accountability and integrity are fundamental to the relationships that enable trade, build society and support economies across the globe. For centuries, the accountancy profession has provided the foundations of business information and trustworthy information exchange. Investors and authorities alike have placed their trust in the audited accounts of businesses of every size. But in the wake of adverse events – from the global financial crisis of 2007–08 to strings of high-profile frauds – public trust in business has suffered, and the spotlight of those seeking someone to blame has turned to the auditing profession.

As business itself responds to the seismic shifts in patterns of production and consumption prompted by the move to digital technologies for everything from stock control and machine tooling to retail sales and the filling of leisure time, the very basis of the relationship between society, the business and the individual is re-forming continuously.

The faith that decision-makers put in information is changing, as the nature of the information and, indeed, of the decisions themselves, is transforming.

The role of the auditor, perhaps never properly understood, stands ripe for evolution in the ever more complex environment of technologically enabled business. There have been and will continue to be debates over the role of audit professionals in fraud detection. As stakeholders' expectations of business respond to global megatrends such as changing demographics, globalisation, climate change and technological advances, so the demands for assurance will develop. Investors and other stakeholders will expect the adoption of appropriate measures in respect of every changing risk. Can a discussion of the internal compliance and regulatory responses help identify areas where, in principle, there may be scope for auditing to contribute more proactively to the internal control environment intended to detect fraud?

DEFINING THE PROBLEM

Estimates of the annual global cost of financial crime vary from US$1.4 trillion to US$3.5 trillion (EY n.d.a.). This wide range is as much a function of the difficulty in defining economic or financial crime as it is of measuring its impact. Beyond purely monetary activities such as bribery and fraud, definitions can include cybercrime and slavery and human trafficking (Refinitiv, 2018). Alongside the initial criminal activity, money laundering is a common factor affecting the stability of the financial system, in turn supporting and facilitating wider damage to individuals and society.

The terms 'economic crime' and 'financial crime' can be used interchangeably,[1] and there are many definitions of economic and financial crime, some based on motive and others on the actors involved. Some distinguish between internal and external threats, and others between the outcomes of the activities. In this report, we focus on common external breaches

[1] 'Economic crime, also known as financial crime, refers to illegal acts committed by an individual or a group of individuals to obtain a financial or professional advantage. The principal motive in such crimes is economic gain' (Europol, 2019).

The frauds relied upon misplaced faith in existing trust mechanisms to persuade innocent victims to transfer money or goods to fictitious or malicious counterparties.

against business that share the common theme of abuse of trust, and may or may not lead to material impacts on the business results. All may have a direct impact on accountants, as they engage and advise clients while the latter will additionally concern auditors.

The abuse of another's trust to persuade them to transfer sums that would not be paid if the true facts were known is the essence of fraud, one of the oldest and most pervasive of crimes. Whether the criminal's aim is to divert value directly to themselves, or to legitimise the use of money already stolen, deceiving the victim into making payments is one of the oldest criminal offences known, as well as one of the most common. Laundering the proceeds of other criminal activity is a widespread threat to the integrity of financial systems. It is a 'pure' economic crime, being predicated on whatever offence created the original proceeds.

Corruption and its close bedfellow, bribery, reach into every country and every sector. A Transparency International survey of 164,000 people found that 25% had paid a bribe in the preceding year (Transparency International, 2017) and 38% of respondents to the 15th EY Global Fraud Survey stated that bribery/corrupt practices continue to occur widely in their country (Gordon, 2019).

The damage done by bribery takes many forms, from the direct disadvantage to a business that is forced to pay more than it should to access goods or services, to the harm suffered by consumers when a business dishonestly buys contracts, putting the business in a position where it can produce substandard or overpriced goods, safe in the knowledge that it faces no competition. In some parts of the world, buildings that collapse during earthquakes are known as 'bribe buildings' and similar infrastructure failings around the world are openly linked to bribery and corruption (Jones, 2018).

'Long firm fraud' was first recognised in the 19th century, facilitated by the creation of long-distance communications (Fraud Advisory Panel, 2018). Relying on the expansion of credit and commerce between different cities and even countries, swindlers would create an impression of genuine trade, perhaps with no more than a forged letterhead, and order goods with no intention of payment.

The frauds relied upon misplaced faith in existing trust mechanisms to persuade innocent victims to transfer money or goods to fictitious or malicious counterparties. The development of the crime followed directly upon the development of legitimate and useful tools for boosting economic activity. In the days of physical written correspondence, long-distance trade was rare and conducted almost entirely between known parties. But as the pace of trade increased, along with the ease of transporting goods and the growth of regular, predictable trade between counties, countries and even continents, so the mechanisms for bringing traders together developed.

ENABLING BUSINESS OR ENABLING CRIME?

Parallel advances in the legal frameworks for businesses played a part. The existence of financial instruments and services far pre-dated the joint stock company, and perhaps the earliest known example of an insurance fraud dates to 300BCE, when a Greek shipowner sought to despatch, albeit empty, a vessel insured for a full cargo of grain, while selling the grain separately (Fraud Advisory Panel, 2018).

> *"Driven by globalization and digitalization, the fraud risk landscape is continuously taking on increasing complexity and velocity. Modern-day auditing professionals are increasingly making use of forensic specialists and technology to identify and respond to these fraud risks."*
>
> **Andrew Gordon**
> **Global Forensic & Integrity Services Leader, EY**

Attempts to abuse these mechanisms range from the creation of fake websites to the registering of false company documents and returns.

The growth in joint stock companies, driven in large part by the UK railway boom of the mid-19th century, presented not just the opportunity for businesses to hold and manage large fixed assets on a long-term basis, funded by the aggregation of surplus capital, but also the opportunity for criminals to exploit loopholes in the legal framework, and misplaced faith in its effectiveness, for their own gain.

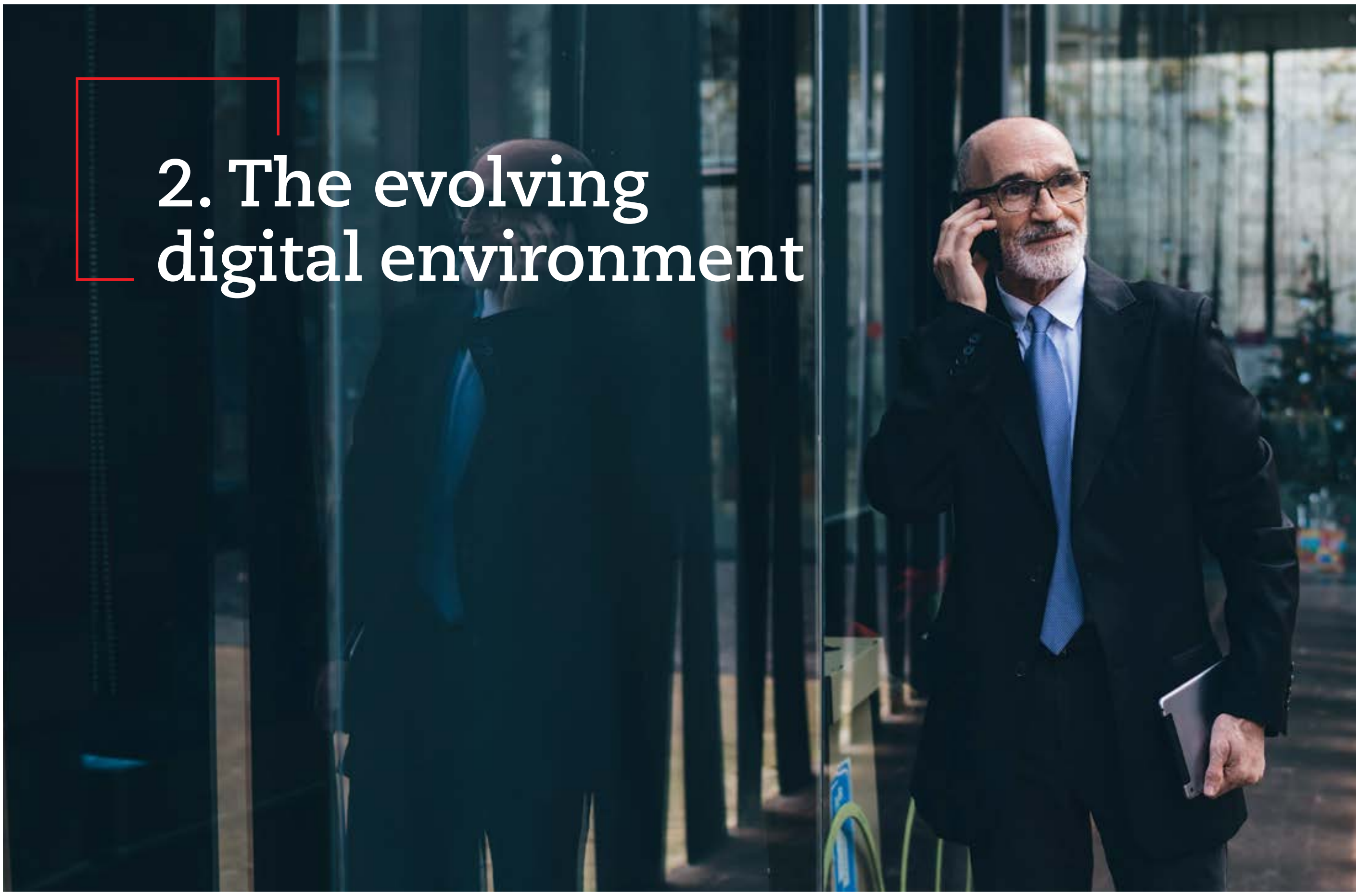
Without technological tools to enable trade at a distance or with strangers, the external trust mechanisms needed in business were minimal. Individuals would trade face to face and disputes would be settled locally. As relationships grew more distant, so trust mechanisms, in the form of courts, banks and agents, grew in importance. The value of an independent opinion, verifying the key financial fundamentals of a business, was reflected in the development of the formal audit profession.

Today, consumers will think little of transacting with a business on the basis of nothing more than a cursory internet search, their faith implicit in the law enforcement, accountability and transparency mechanisms that have grown up in parallel with the growth in trade. Attempts to abuse these mechanisms range from the creation of fake websites to the registering of false company documents and returns (for example, claiming falsely that the business has been audited by a well-known firm).

The scope for technology to affect transactions of every kind became increasingly apparent around the turn of the 21st century. The extent to which business was starting to rely on digital communications tools was highlighted by the LoveBug and Melissa viruses, which exposed a wide range of weaknesses in approaches to protection and exploitation of the potential benefits of the new tools. Even so, the benefits and legitimate uses of technology far outweighed the risks posed by its abuse.

In the rest of this report, besides references to extant research literature, you will find a number of comments by forensics, technology and compliance professionals consulted by ACCA for their knowledge and experience in helping organizations prevent and detect economic crimes. A full list of these appears on page 21.

> *"We are only scratching the surface of what AI and data analytics technologies can do to help prevent and detect fraud. However, they are a means to an end. As organizations invest in greater technology adoption, they need to bear in mind that the ultimate goal is to drive better insights and transparency, and having a sound and secure data strategy is the key to achieving that goal."*
>
> **Todd Marlin**
> **Global Forensic Technology Leader, EY**



2. The evolving digital environment

The development of economic crime has progressed in parallel with the development of trade and business technologies. As value transmission moved from barter to financial instruments, and the relationships between traders became ever more remote and reliant on intermediaries, so the scope widened for abuse of the enabling mechanisms that underpin effective trade.

But has the step change in business technology effected by the digital revolution had a similar impact on the commission, detection and prevention of economic crime?

TRUST AT A DISTANCE

As technology advances, so the scope for supplementing or even replacing existing trust mechanisms with technological tools has expanded. Perhaps the most high-profile attempt to replace external human accountability mechanisms with internal technological ones so far has been the Ethereum decentralised autonomous organisation (DAO). In 2017, a blockchain-based smart contract was launched, crowdfunded entirely in cyberspace and deliberately divorced from every existing framework, having no registered existence, no contracts enforceable in any recognised jurisdiction, and no reliance on an existing fiat currency (Waters, 2016a).

The limitations of this model were swiftly revealed when a feature of the code enabled one investor to siphon off a significant portion of the investment to their own wallet, entirely contrary to the intentions of the other investors and apparently the founders. Where minority investors in a registered corporation would, in most jurisdictions, have had recourse to the courts, there was instead recourse only to the code, and to the investors' apparent agreement with the outcome when that code was executed (Waters, 2016b).

The incident raised fundamental questions about whether a crime had actually been committed, given the apparent agreement of all participants to be bound by the features of the code. What is clear, though, is that the ultimate beneficiaries of all businesses are individual people and, for the time being at least, it seems that policing the regulation of business relationships is also ultimately a human responsibility.

In commission of such relationship-based crimes, our panel of interviewees are unanimous that digitalisation has led to an increase in the volume and velocity of economic crime attacks, as well as an expansion in scope.

Historically, 'cold call' frauds would have been carried out by letter or by phone, with corresponding linear resource costs for the perpetrators. Mass mailing and the availability of harvested lists of email addresses have hugely increased the number of victims that a scammer can target in a single attack. As Anthony Harbinson, Director of Safer Communities, Northern Ireland,[2] observes, 'If you send out one thousand emails and only one comes back, that one could get you significant amounts of money'.

The existence of underground chat rooms and encrypted communications, meanwhile, has enhanced criminals' ability to exchange and refine ideas. Harbinson notes that '[I]f you go on to the dark web, you can actually buy for anything from $5 to $55 a range of templates that you can send out to any organisation that look specifically like their own templates, except it will relate back to whatever bank account or address that you actually put on top of it'. Patrick Craig, Partner and EMEIA Financial Crime Technology Leader, Ernst & Young LLP United Kingdom, warns that:

[2] A full list of the panel of experts can be found at page ⍰⍰

> Applying similar machine learning techniques to phishing emails can improve their criminal efficiency, while the use of AI to create 'deep fake' videos has raised concerns about the risk of identity theft.

'To recruit an army of virtual agents to carry out attacks, you can buy malware, networks of compromised machines and mule accounts from the dark web to enable money laundering needs, versus recruiting a human army to help launder the proceeds of crime'. New technologies are allowing even criminals who lack the skills to design an authentic-looking fraud to pose a significant threat to their targets.

THE GLOBAL VILLAGE

Online trade allows businesses to reach new markets, whether within their own country or abroad. Similarly, consumers can benefit from wider choice, as the chance to browse catalogues online without having to visit a showroom expands the number of suppliers they can consider. Secure digital payment technologies have taken the apparent risk out of online ordering, while the potential for ordering from another country has massively increased.

Business has not been slow to capitalise on this, with many larger suppliers taking the opportunity to route trade through regional hubs, often for their own regulatory, logistic or, in some cases, tax reasons, so that consumers have become accustomed to foreign addresses and company details on sales documentation. Just as the internet and World Wide Web have freed legitimate business from the shackles of geographical location, so crime too has been able to operate across borders.

Criminals have used the same tools to expand the geographical reach of their operations. The cost of sending a cross-border email is no greater than that of sending it next door. Cross-border online communications do not impose the same cost burden on the perpetrator that conventional communications do, and there are other advantages to the criminal. Many consumers might be wary of a foreign postmark on their mail, or a foreign accent on a cold telephone call. But spoofing of email or web addresses, and use of native-speaker-reviewed documentation, can remove all these warning signs from an online attack.

Rather than vast criminal empires, some regulators are seeing the development of online fraud as a modern-day cottage industry, with large numbers of criminals deploying similar tactics simultaneously. The dispersal of criminal knowledge and techniques broadens the base on which they can draw to share refinements, or warn of effective defences that have been developed or encountered.

Rachel Sexton, Partner, Ernst & Young LLP United Kingdom Forensic & Integrity Services, has noticed a shift in behaviour: 'I think technology has allowed criminals to sit remote from their victims. We see attacks coming from all over the world, for example, targeting UK banks. It does make it much more sophisticated, that the criminals can sit somewhere else and make these attacks and remain relatively anonymous'.

Many consumers prefer to communicate by text, rather than on the phone. Scammers have noted this, and use chatbots to spread their wares. Chatbots based on artificial intelligence (AI) can automate the entire process of tricking users into infecting their own machines, or handling the communications associated with ransomware. Applying similar machine learning techniques to phishing emails can improve their criminal efficiency, while the use of AI to create 'deep fake' videos has raised concerns about the risk of identity theft (Fintech Times, 2019).

A further development, which affects not only the efficiency of the criminals' operation but also the difficulty of tracing them, is the massive increase in the power of mobile devices. Operations that only a few years ago would have required substantial fixed plant, even to carry out an entirely online scam, can now be effected through a mobile phone, or at most a laptop, toted from one internet café to another.

Correspondingly, the rise of bring-your-own-device (BYOD) policies and the blurring of lines between personal and business online personas has changed the defence perimeter. It is no longer enough to police the business network;

The ability to transfer value anonymously has huge implications for both money laundering and the broader fields of economic crime, such as people trafficking.

the device and user are the key elements in any digitally enabled economic crime cyber attack. The routes may have changed, but the fundamentals of breaching personal trust remain central to the commission of the crime. The ease with which criminals can compromise email domains and create convincing communications shifts the burden of detection back onto the individual.

As well as the simple proliferation of existing crimes, technological developments have introduced new vectors for crime. The development of cryptocurrencies and their availability as mechanisms for storing or transmitting value in an anonymous or pseudonymous fashion have transformed some aspects of economic crime. Nonetheless, conventional business fraud seems, for the time being, likely to continue to be carried out using fiat currency. As Claire Jenkins, Forensic Accountant, puts it, 'I think then the question is: how comfortable would someone be doing businesses with an individual [who] wants you to pay him entirely by cryptocurrency? Is it likely, even now that people will accept the payment? I have my doubts'. While the majority of respondents to the EY Global Fraud Survey 2018 stated that their organisations would soon be regularly using digital payment systems, just 4% expected to be conducting business using cryptocurrencies (EY, 2018a). But in situations where trust is already compromised, the picture is very different. The ability to transfer value anonymously has huge implications for both money laundering and the broader fields of economic crime, such as people trafficking.

The initial assumption of many people that early blockchain-based cryptocurrencies were impossible to track is widely recognised as no longer being true (Emerging Technology from the arXiv, 2017). While bitcoin, Ethereum and the like remain popular for many criminal transactions, they have been superseded by purpose-built anonymous currencies for those who are determined to remain untraceable. The use of tumblers, which mix 'dirty' and 'clean' cryptocurrency funds to hide the traces of the source and destination of funds, is a recognised threat to accountability. The ability to purchase goods on the dark web via genuinely untraceable funds has clear implications for terrorist financing.

There are further issues when dealing with cross-border criminal activity. The use or ownership of cryptocurrencies in China has been outlawed, in part as a response to their use as a mechanism for evading exchange controls. In addition, there is a clear risk of breaches of sanctions regimes. In addition to the attraction of making anonymous transfers to those subject to sanctions, financial institutions with regulatory responsibilities under those regimes now face the threat of inadvertent breach if they operate using such cryptoassets. The instant a transfer is made, receipt of the funds could trigger liability, yet it is inherent in the nature of the asset that the recipient entity cannot undertake due diligence in the conventional sense.

The difficulty of tracing cryptocurrency transactions, allied with the ease of accessing them, has 'fuelled secondary markets for criminal activity', warns Narayanan Vaidyanathan, Head of Business Insights ACCA. 'And the reason they've been able to fuel that is because they have this inability to directly track and trace the beneficial owner of the funds. And that's a challenge that we did not have in the same way previously'.

The implications of that challenge can be immense. In one instance, a teenager took advantage of the ease of access to online tools to purchase a distributed denial of service (DDoS) attack, which he targeted at his school's website so as to create a plausible excuse for playing football with friends instead of completing and submitting online homework. In fact, the prank backfired: the school's site was hosted by the internet service provider (ISP) that supported the transport provider for the UK's organ donor network, and the attack disrupted vital surgery across the country.

> The usefulness of customer lists to direct competitors has long been recognised, but increasingly it is simply the personal information held by a business that motivates criminals to attack.

NEW HORIZONS

That incident also relates to the evolution of existing economic crimes. Technological advances are creating entirely new forms of attack on the value inherent in businesses. Denying a business access to its markets would have been historically uneconomic for criminals to consider, yet the disruption caused by a DDoS attack on an online seller can now be generated for minimal cost, and at low risk. The modern-day protection racket is more likely to arrive via email than in an anonymous car full of heavyset men with baseball bats.

Keeping records and managing data have always been fundamental to successful business decision-making. Auditing, and the trust that it creates for stakeholders, relies on manageable and trustworthy data. But the digital era has brought more data than ever, in both volume and variety. There is an opportunity here for accountants to derive an even greater advantage from the increasing data by generating better insights and extracting the maximum value from the resource. To this end, accountants can work with compliance and risk departments to identify risk areas and can help assess the effectiveness of the controls in place.

On the other hand, this opportunity for legitimate business has a mirror in the criminal world. The usefulness of customer lists to direct competitors has long been recognised, but increasingly it is simply the personal information held by a business that motivates criminals to attack. In addition, for the newer-platform business models, the value of network effects[3] is an essential element in their attractiveness to partners – and criminals.

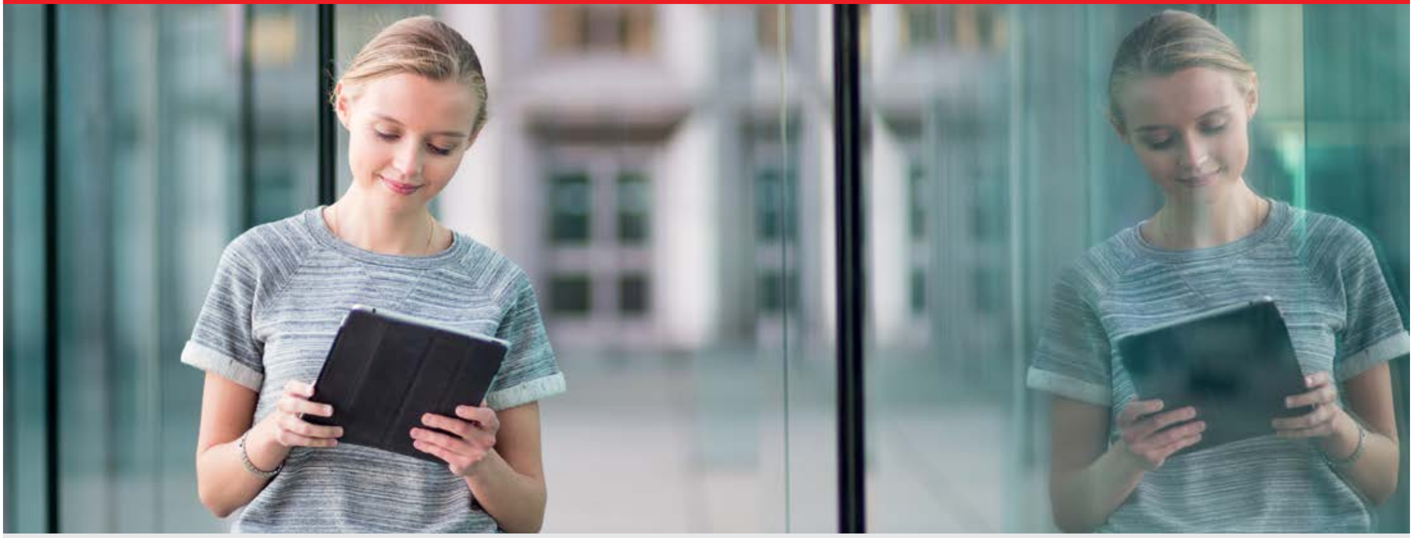
Working out where in the matrix of economic crime such activities fit will be a challenge which informs the regulatory response. Arguably, in a spectrum that ranges from fraud through money laundering and even possibly encompassing human trafficking, there is a place for the deliberate targeting of a business's revenue-generating machinery as a means of generating revenue for thieves.

Facing the increasing complexity of fraud patterns, there are many technology tools that have been more widely adopted by forensic accountants to identify risks and investigate criminal activities more effectively and efficiently. At the same time, some jurisdictions have been seen as effective in encouraging the private sector to explore new technological methods of creating value and combating economic crime. For example, Jack Jia, Partner, Ernst & Young – Hong Kong Forensic & Integrity Services, notes that: 'the [Hong Kong] Government does recognise that technologies are changing. They embrace technology and encourage FinTech … In Hong Kong, there are various regulators [that have] set up sandboxes and chat rooms to allow FinTech companies to … trial out new technology that could benefit the communities'.

> *"Economic crime may sound like an age-old topic on the surface. Underneath it, new fraud vectors and players emerge all the time. As you tirelessly chase these new risks, you may be better off by taking a pause to assess whether it's time to take bigger leaps to transform the way you deploy people, process and technology."*
>
> **Jeanne Boillet**
> **Global Assurance Innovation Leader, EY**

[3] 'Network effects' is a term describing the non-linear relationship between the increase in number of nodes (users) in a network and its effectiveness and value for network members. Increases in a network's size disproportionately increase its value.

Do it faster, do it smarter, do it leaner



'Artificial intelligence (AI) applies advanced analysis and logic-based techniques, including machine learning, to interpret events, support and automate decisions, and take actions.' (Gartner, 2019a)

'Forensic data analytics (FDA) is the collection and analysis of all types of data, structured and unstructured, with the objective to manage legal, compliance and fraud risks. When enhanced through human intelligence, companies can use FDA technologies and techniques to better monitor, prevent, etect, investigate and predict anomalies in business activities and transactions.' (EY, 2018b)

BELOW IS A LIST OF AI AND FDA TECHNOLOGIES AND TECHNIQUES THAT HAVE BEEN INCREASINGLY USED IN FRAUD DETECTION AND COMPLIANCE MONITORING.

Rules-based descriptive tests – by using historical data with simple and complex analytical-weighted tests, significant value can be achieved in identifying areas of risk. Alerts will be produced when a specific condition is met. For example, if an employee submits an expense for reimbursement of an amount in excess of a predefined reimbursement policy, then an alert would be triggered. These types of analytics are often easy to implement as they rely on predefined conditions and policies. For this reason, this is the most common FDA technique used by businesses.

Topic modelling and linguistic analysis – these tools use text analytics to identify suspicious phrases, high-risk topics or unusual patterns of behaviour in the free-text components of the data. Beyond keyword searching, topic modelling seeks to cluster, quantify and group the key nouns or noun phrases in the data, enabling the investigative team to gain a rapid understanding of what information may have been compromised or the corrupt intent of certain business activities. Linguistic analysis techniques use the results of text analytics to identify the emotive tone of the communication – identifying anger, frustration, secretiveness, harassment or confused emotions, among other sentiments.

Statistical analysis and machine learning – this technique leverages historical facts in the data and uses machine learning to make predictions about future or otherwise unknown events. The incorporation of statistical models into this approach further increases the confidence that items identified as outliers warrant additional review, thus limiting the amount of false positives and increasing the efficiency of the review process.

Data visualisation and link analysis – data visualisation, including heat maps, geospatial analysis, time series analysis, word cloud and stratification, enables the identification of trends and outliers in one interactive dashboard. Threats and hidden relationships across data sources are aggregated, extracted and prioritised for evaluation and subsequent in-depth investigation, if warranted.'

Robotic process automation (RPA) – this is a productivity tool that allows a user to configure one or more scripts (which some vendors refer to as "bots") to activate specific keystrokes in an automated fashion. The result is that the bots can be used to mimic or emulate selected tasks (transaction steps) within an overall business or IT process. These may include manipulating data, passing data to and from different applications, triggering responses or executing transactions. RPA uses a combination of user interface interaction and descriptor technologies. The scripts can overlay on one or more software applications (Gartner, 2019b). ■

> The potential for criminal enterprises to create a separate legal personality to execute their operations entirely automatically, and dissolve it once done, cannot be ignored.

There is one final development that cannot be ignored. When thinking about the types of crime seen in people's daily work, the evolutionary nature of change is a common theme, as is, in particular, the human aspect of all the crimes. In every case, the protagonist is human, and in all too many cases it is the corruption of the human decision-making process that is essential to the success of the criminal venture.

Increasingly, AI has the potential for automating not just processes but also decisions. The value of AI as a decision-support tool is well documented. For instance, use of AI to support clinical decision-making in the health care sector is widespread (Sullivan, 2018), and the recognition that the ultimate diagnosis rests with the human medical professional is well established. But increasingly, algorithms are taking on the role of a decision replacement mechanism, initially more so in cases where structured data plays a significant role in the process, as regulatory concerns (and management concerns) may be easier to address here. For the AI tools themselves, however, there is no difference between structured and unstructured data and, as the regulatory environment and management attitudes evolve, so too we can expect more widespread and comprehensive adoption of the technology.

A number of loan platforms and banking providers use AI credit-scoring mechanisms, while pricing structures for ticketing apps are common candidates for automation. But where the entire decision-making process is automated with no human oversight, who bears responsibility – and how can the effectiveness of the outputs be measured?

Craig identifies some of the risk areas: 'What are you training these models on? You're training them on historical investigations. You get into all of the biases of historical decisions. There's a huge field of AI and ethics that needs to be considered around the use and application of these technologies so that you're not getting into some quite harmful unintended consequences'.

Reports are already emerging of AI decision engines reflecting and reinforcing historical patterns of discrimination in everything from bail applications (Simonite, 2019) to credit-limit scoring (Cox, 2019). The German airline Lufthansa faced reputation management issues after an AI pricing algorithm appeared to increase prices significantly in response to a competitor's bankruptcy (Matthew, 2018). Businesses that seek to rely on AI for decision-making must address the risks of inadvertently breaching the law. New York State Law, for example, requires financial products and services offered in the state not to discriminate against protected groups. If, as has been alleged (Cox, 2019), some payment card limits are discriminating against women, then this would expose the card issuer to liability.

As businesses recognise and respond to the potential for regulatory action on, or consumer responses to, these issues, there will be scope for accountants to work with compliance and internal audit teams to identify those risk areas proactively. The capacity for assessing the effectiveness of the controls in place, and reporting on that effectiveness to interested stakeholders, can produce a firm foundation of objective evaluation on which to build trust in the new tools.

The ability of automated tools to implement their own decisions raises further possibilities. The creation of incorporated legal personalities is increasingly an online process and susceptible to automation. The potential for criminal enterprises to create a separate legal personality to execute their operations entirely automatically, and dissolve it once done, cannot be ignored. As the risk grows that AI could be an enabler of criminal activity, the question arises as to where the responsibility for those acts would lie. 'The nature of economic crime is not just about the crime itself. It's also the evolving age of accountability for the crime', notes Narayanan Vaidyanathan. How will the legal frameworks, built on human ethics and responsibility, respond to this entirely novel challenge?

3. Policy and practice: responses to economic crime in a digital age

Opportunities for business and society in this new digital landscape are clear – from the ease and simplicity of a cashless society to the consumer benefits arising from FinTech. Nonetheless, as Chapter 2 demonstrates, these changes in commercial practice also provide new opportunities for criminals in the economic sphere.

Given the changing technological landscape, ACCA and EY have explored the evolving role of the regulator, other government institutions and accounting professionals in combating economic crime in the digital age. A clear point arose from these discussions: professionals interviewed for this report agreed that the overall objective of regulation, and the historic tensions within industry and innovation, have not changed. There is still a pressing need to create a regulatory environment that supports financial innovation, while at the same time limiting the risks for consumers and businesses, supported by audited information to inform decision-making. Auditors could assess whether a company has adequately put in place controls to comply with the sector-relevant laws and regulations in the jurisdiction in which it operates. These laws and regulations would not only be those relating, for example, to money laundering, corruption and tax evasion – but also those concerned with data protection, environmental impact and the treatment of the workforce, among other concerns.

But Vaidyanathan noted: 'there's an issue, as there always is, around balancing regulation and innovation … that it's impossible to create laws to cover each and every scenario'.

ALWAYS A STEP BEHIND

There was widespread agreement among those consulted that policymakers and regulators must tackle the evolving nature of economic crime in a digital age from a position of disadvantage. David Higginson, Partner, Ernst & Young LLP United Kingdom Forensic & Integrity Services, described 'a lag between how technology advances, which [is] so rapid, and the law catching up'. This view was commonly expressed by interviewees across ACCA and EY networks. This lag will be exacerbated by the skills and knowledge deficits within the regulatory community, where Mark Le Page, Director, Ernst & Young LLP United Kingdom Advisory, notes 'the problem fundamentally is that nobody really understands the technology or the implications of the technology'.

Certain realities of public institutions can reinforce this lag between technological development and regulation. For example, Nick Maginot, Partner, Ernst & Young – Australia Forensic & Integrity Services, notes that governments 'are, by their very nature, reactive and at the whims of their stakeholders'. A high-profile economic crime may produce significant pressure for a harsh regulatory response, whether or not this is considered effective by experts. In addition, governments must consider the needs of a variety of citizens in the provision of public services and in setting out regulatory requirements. For example, the ability to keep either paper or digital records, a rule made to accommodate organisations that are not digitally sophisticated, can complicate enforcement activity. Scott Jarrell, Partner and Forensic Data Analytics Leader, Ernst & Young LLP United States Forensic & Integrity Services, cites the example of Bernie Madoff, who produced detailed paper records for his Ponzi scheme to comply with regulatory requirements.

> "Cryptocurrency has fuelled secondary markets for criminal activity [because] of this inability to directly track and trace the beneficial owner of the funds. And that's a challenge that we didn't have in the same way previously."
>
> Narayanan Vaidyanathan

In this difficult context, governments and enforcement agencies need to consider the new policy challenges that arise from this digital age – as well as the best ways of responding. Enhancements could include audit attestation as to compliance with regulations, not only in financial areas such as tax or anti-corruption measures, but also in developing fields such as data protection and cybersecurity. As tools develop, the assurance could expand to other fields of growing importance to stakeholders, such as supply chain assurance over people trafficking or conflict minerals, building social as well as financial benefit.

POLICY CHALLENGES – ANONYMITY, ACCESSIBILITY AND ACCOUNTABILITY

For regulators and policymakers, economic crime in a digital age presents some particular challenges in addition to those dealt with before. These include, at a minimum, challenges pertaining to anonymity, accessibility and accountability (Figure 3.1).

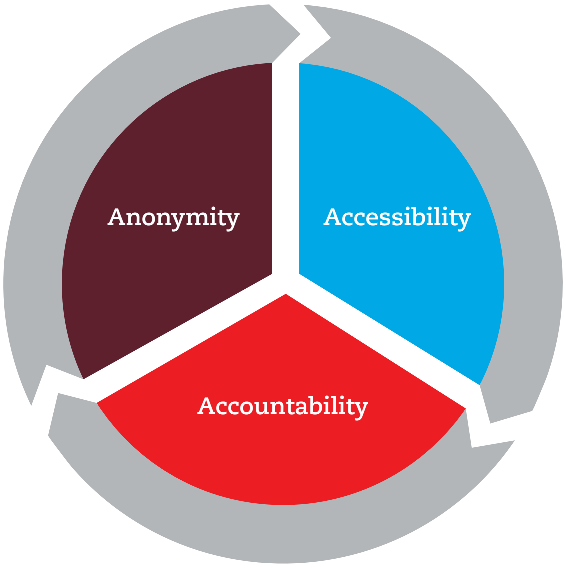
Anonymity

Transacting through the online environment has provided avenues by which fraudsters can avoid disclosing their identity or provide false identities. The idea of opaque fund holdings or complicated financial structures to obfuscate the view of regulators is not new in itself. And cash is, of course, the classic tool for facilitating untraceable, 'under the table' payments.

Now, the anonymity associated with cryptocurrencies adds a new method for facilitating payments. These currencies are anonymous by design (or pseudonymous, to be more exact). In other words, it is possible to see the target addresses to which funds are going, but this does not provide a reliable confirmation of the identity of the actual counterparties or individuals in the background. As a result, observes Vaidyanathan, we see that 'cryptocurrency has fuelled secondary markets for criminal activity [because] of this inability to directly track and trace the beneficial owner of the funds. And that's a challenge that we didn't have in the same way previously'.

For certain cryptocurrencies, it may be possible to isolate the identity of the individual involved, for example, by linking activities across various transactions to establish patterns of behaviour. But this is not always possible, and not a guarantee of establishing identity. Furthermore, there are many cryptocurrencies that have been developed specifically to prevent this. These have sophisticated mechanisms that ensure a lack of traceability and might use, for example, 'stealth' addresses that make it difficult to check where the funds are going, or anonymising the internet protocol (IP) address associated with the transactions. Le Page cited the ability of financial criminals to 'exchange without trace' as a serious challenge for government – creating a new environment of 'crypto-anarchism'.

FIGURE 3.1: Policy challenges arising from the digital age



This increased anonymity creates new challenges for policymakers, regulators, compliance and audit professionals working to tackle activities such as money laundering.

This increased anonymity creates new challenges for policymakers, regulators, compliance and audit professionals working to tackle activities such as money laundering. The related challenge of KYC lies at the heart of dealing with this issue. It is already a space keenly contested between those committing crimes and those seeking to catch them – and this will intensify as a key battleground for the future. It was in this context that Higginson rightly notes that 'the ability to identify and do proper KYC checks quickly and efficiently is still the holy grail of a financial crime compliance department'. The sheer number of information sources now available about one's customers can lead all easily to what Glenn Perachio, Partner and Forensic Technology Leader, Ernst & Young LLP United Kingdom Forensic & Integrity Services, describes as 'alt-tab syndrome or the swivel chair compliance officer', a risk that can be countered by effective use of RPA and related technologies.

In addition to design features such as those described above, anonymity is also helped more broadly by the sheer speed of financial transactions using digital systems. If funds can be digitally moved in and out of accounts at great velocity, it makes it more challenging for compliance departments and auditors to know with certainty that they are being presented with a credible version of the reasons.

Sexton's experience is that 'technology also helps [criminals] move the money quickly once it's been stolen. We've seen money being stolen from bank accounts, or also cryptocurrency being stolen, and the speed at which you can move these funds means it makes it very difficult for law enforcement to then try to recover the funds, or for the banks to try to freeze the accounts'.

Therefore, the increasing velocity of movement of fiat money, facilitated by the new digital environment, creates challenges for banks attempting to put a stop to nefarious transactions, but these challenges are compounded by the increased anonymity made possible by cryptocurrencies.

Accessibility

Financial crime has become a more accessible activity, with experts identifying reduced barriers to entry for undertaking a financial crime, the proliferation of information on the internet and many of the perpetrators conforming to stereotypes of the 'hardened criminal'.

The marketplace characteristics of the digital crime mean that it may be possible, for example, to hire the services of cybercriminals even if one does not know how to commit the crime oneself. This level of accessibility does not presuppose any connection to the world of cyber hacking or the need to have an extensive network of contacts or knowledge in the area. Craig highlighted that 'you can have a 14-year-old in their bedroom download[ing] malware and recruit[ing] a botnet to take part in a sophisticated attack, perhaps unknowingly to some degree. There's a worrying aspect of "gamification" to cyber attacks'.

This is a substantial evolution for regulators and law enforcement, compliance and accountancy professionals – as well, of course, as the victims of these crimes and potentially everyone who works in or has dealings with financial institutions. Clearly, public bodies will require additional resources to match this potential proliferation of digitally enabled economic crime.

Another facet of the accessibility challenge is the significant increase in cross-border activity or the globalisation of economic crime. Regulation, even in the 21st century, is jurisdictional in nature. That jurisdiction may be a country, or in some examples, a group of countries collaborating under a common regime, but it is still not a unified global approach.

'The big difference is now the cross-jurisdictional aspect of these crimes. Beforehand, these frauds would have been carried out on a local and national level. They are now being carried out on an international level. You are as likely to be scammed from Jakarta, as you would be from Kiev, as you would be from any one of the islands within the Philippines', warns Harbinson.

There is a challenge here in ensuring proportionate and fair regulatory and associated regimes that will allow innovation to flourish while providing essential safeguards for accountability.

Therefore, the challenge is that the criminals operate across jurisdictions in a seamless way using the power of the internet. The locations of a criminal and their target could be in completely different jurisdictions, whose law enforcement agencies have no interaction with one another. This unprecedented access to a global pool of targets has given economic crime a previously unthinkable level of scalability. And the regulatory challenges to dealing with this are significant because it is difficult for government agencies to coordinate across borders at the same speed as the perpetrators of crime.

As Maginot tells us, 'Criminals and the nature of the criminal activity [are] inherently cross-border. Crime does not recognise borders: it only looks for the clearest path to a successful criminal outcome'.

Accountability

The digital age presents difficult questions of judgement, given the sophistication of some of the technologies involved. Algorithmic models, for example, can be complex and it may not be easy for compliance departments or the regulators providing oversight to understand how and why these models are performing in a certain way.

This, however, should not become a reason for corporate actors to absolve themselves from responsibility. Ultimately, legal structures as they stand look at a legal 'person' as being an individual or corporate entity. The implication is that human oversight cannot be dispensed with by simply outsourcing responsibility to an algorithm.

'It's great that we have algorithms that can help review false positives, or identify suspicious activity, or flag fraudulent activity or patterns. But it is difficult to rely completely on them because if they do not flag money laundering or dismiss a false positive, the risk remains with the firm', says Sexton.

The important challenge here will be to achieve the right regulatory balance between human oversight and reliance on the machine. Getting this wrong could create a wider discontent among organisations in that when things go well, the technology gets the credit, but when things go wrong, the individual gets the blame. There is a challenge here in ensuring proportionate and fair regulatory and associated regimes that will allow innovation to flourish while providing essential safeguards for accountability.

This is the reality of augmented or assisted intelligence, rather than full AI. Should regulatory or legal responsibility be applied differently in the case of a flawed credit model that is intentionally manipulated for fraudulent intent as opposed to one that is unintentionally fed with biased data input? Having an appreciation of this requires some level of granularity in regulators' understanding of technological development and how that translates to issues of accountability and integrity.

Sexton notes that, 'Companies cannot hide behind faulty technology implementation. When things go wrong, [they] will bear the regulatory, financial and reputational harm as a result of it'.

> *"The role of professional accountants is to help create a better world. Every crime has a human origin, and a human cost. As technological advances reshape the world we work in, the approach to tackling crime and corruption will have to evolve with both the threat and the countermeasures"*
>
> **Helen Brand**
> **CEO, ACCA**

The availability of advanced AI and forensic data analytics tools allows businesses to go far beyond simply identifying single illicit payments.

CORPORATE AND REGULATORY RESPONSES: A SPOTLIGHT ON GOOD PRACTICES

The impact of the digital age on the detection and prevention of crime is equally relevant when exploring the possible responses by regulators, companies and government enforcement agencies. A series of good practices, which can be applied in working to improve the detection and prevention of economic crime in a digital age, were identified by our interviewees and are explained below.

Applying new technology to detect and prevent economic crime

The professionals interviewed for this report were unanimous that as well as creating the opportunities for abuse, new technology can aid in the fight against crime, in both detection and prevention.

The use of AI and forensic data analytics to enhance risk assessment in banks and financial institutions has significant implications for the effectiveness of anti-money laundering (AML) and sanctions controls. In addition, the application of RPA will allow for the streamlining of operations and enhanced consistency, while alleviating compliance and auditing professionals from routine, rule-based tasks and enabling them to focus on high-risk areas. Cross-checking of identity details for account verification can be undertaken quickly and cheaply enough to improve security without unduly compromising customer experience, raising the prospect of achieving Higginson's 'holy grail' (see 'Anonymity' above).

Equally, the analysis of expense account expenditure in sales teams could aid in the identification of bribery or of facilitation payments made outside company policy. Harbinson sets out the concerns that, 'If you start getting large amounts of money being spent on bars, hotels, restaurants, strip clubs, … there should be someone looking and confirming: Is that real? Is that allowable?… If you give a credit card to someone, a hospitality account to someone, what are they using it for? And is the organisation either knowingly or unknowingly breaking the [law]?'. Beyond this, more focused tools can assist with due diligence and investigation. Custom applications can be used to perform due diligence and conduct investigations by taking into account unique sector-, geography- or organization-specific risks.

The availability of advanced AI and forensic data analytics tools allows businesses to go far beyond simply identifying single illicit payments. The ability to analyse unstructured data alongside structured data sources and integrate the findings using behavioural and social networking analytics allows employers, within the bounds of local privacy laws, to combine other techniques, such as predictive modelling, audio analytics, text mining and geospatial analysis, to build a comprehensive picture of risk indicators to guide those escalation decisions and target interventions where they will be most effective (EY, 2016).

Nonetheless, while these tools can be useful internally for an organisation, their use in combating the new cross-border development of economic crime can be more problematic. Many jurisdictions impose restrictions on data transfer, potentially posing a challenge to businesses in cross-border transactions where they need to interrogate data sources. Developments such as homomorphic encryption, which allows the interrogation of encrypted data at a distance without the need for cross-border transfers, could enable the use of the full range of analytical tools.

Widespread deployment of technology such as zero-knowledge proofs, allowing for the verification of encrypted information, and self-sovereign identity, which verifies an individual's identity without the need for extensive data transfer, could reduce still further the need for data aggregation within businesses. Without the need to hold large archives of potentially valuable information in reusable form, the attractiveness of business as a target for criminals would decline.

At the level of sector collaboration, the interviewees described the need for regulators and financial institutions to work more closely together in collectively tackling economic crime.

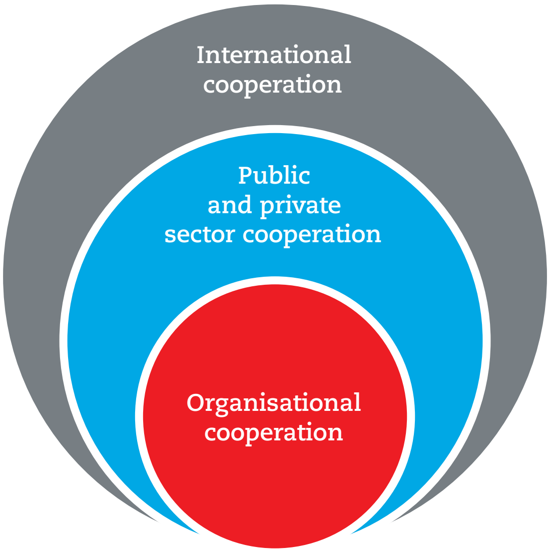
Collaborating for improved detection and prevention

A common recommendation by interviewees was the need for information sharing and institutional collaboration. They described this response at a variety of scales – starting with cooperation between regulators and individual companies, up to the level of international cooperation. This was often described as a more effective response to economic crime than a traditional sanctions regime; supporting a culture of cooperation between institutions and companies was seen as more effective than merely applying penalties. As Anne McCormick, EMEIA Public Policy and Network Engagement Leader, Ernst & Young, notes, 'Auditors have a role to play, but are only one element of a much wider ecosystem'. Figure 3.2 sets out the different scales of information sharing that were identified by the cyber executives as important in improving the detection of economic crime.

At the level of organisational cooperation, Jarrell noted that improvements are still required in how companies share information internally across departments. He stated that, 'historically, a lot of financial institutions have operated in silos [and] being able to cross-reference data in some sort of cross-company [way] should become more important'. A 2015 report from EY and Chartis concludes that, 'What will be needed, therefore, is an integrated approach to the management of financial crime risk and compliance that will help [with] better detect[ion of] criminal attacks and fraud'(Chartis and EY, 2015).

At the level of sector collaboration, the interviewees described the need for regulators and financial institutions to work more closely together in collectively tackling economic crime. Maginot noted that, 'the goals of the regulators are often directly in line with the goals of private enterprise. If it's money laundering, the regulators don't want money laundering, the banks don't want money launderers using their institutions, and so the better they can work together and share information and get information back from the regulator… [the] more effective [they will be] from a preventative perspective'. He also offered the case example of Fintel Alliance, a public–private partnership that seeks to fight serious crime and terrorist financing in Australia (AUSTRAC, 2019). Craig similarly raised the work of the Australian Transaction Reports and Analysis Centre (AUSTRAC) with the Fintel Alliance, citing 'the benefits of how public and private sector work together to improve the overall effectiveness of the regime to detect and prevent financial crime through intelligence sharing'.
There are clear benefits from supporting real-time information sharing across sectors to aid the detection and prevention of crime – but there are also challenges in achieving this seamless

FIGURE 3.2: Scale of cooperation required for effective information sharing


International cooperation
Public and private sector cooperation
Organisational cooperation

Finally, interviewees noted that the expansion of cross-border crime requires a similar scale of response by regulators and law enforcement.

sharing of information. For example, Le Page notes that some regulators, such as the Financial Conduct Authority in the UK, also have a competition mandate. Therefore, there were concerns that any information sharing across sectors and financial institutions must have due regard for commercial concerns, such as the protection of intellectual property. Equally, Le Page notes that the desire to collaborate openly on the common purpose of minimising economic crime has made this a surmountable challenge.

Finally, interviewees noted that the expansion of cross-border crime requires a similar scale of response by regulators and law enforcement. Sexton is clear that 'there needs to be a very joined-up approach between public and private sector[s]. But also, because financial crime is very global now as well, it is not [occurring just] within one jurisdiction or even within the EU, for example. It spans many different jurisdictions'. Effectively tackling transnational economic crime requires a similar scale of response by governments and law enforcement. A key message from across ACCA and EY Small and Medium-sized Enterprises (SME) Network was the need for governments and financial institutions to work together in tackling this increasingly global threat.

'[Money is] hard to recover when it goes into another jurisdiction because the jurisdictions are quite fragmented in how they work together to freeze funds or do asset seizures. It takes so long to work through all the jurisdictional differences. By that time, the money is just too far gone in[to] a secrecy jurisdiction', said Sexton.

The right to individual privacy is a clear barrier to open information sharing recommended by all the above stakeholders. Maginot states, 'the data privacy laws that we have now, and GDPR [the General Data Protection Regulation] in particular, are making [information sharing] more difficult'. There is clearly a need to reconcile state intervention in individual privacy, as well as information sharing across institutions without consent, with the variety of new challenges posed by economic crime in a digital age. Vaidyanathan pointed to the need for 'principles that will support good practices', where the UK has taken positive steps in this area 'by setting up … the Centre for Data Ethics and Innovation'. This centre is tasked with developing the right governance regime for data-driven technologies (gov.uk n.d.). At the same time, the challenges of data protection and privacy were not limited to European organisations that must adhere to the GDPR. Jack Jia explained that the 'sharing of data to third parties or using data to perform additional analysis [can be] a challenge. Say a bank is worried about certain credit card transactions, they want to send the credit card transactions to a third-party data analytics firm to perform the review. Transferring of data to third parties can be a breach of data privacy'.

> *"Regulators, law enforcement and business all have a common interest in combating economic crime. There are huge gains to be made from a cooperative approach to the opportunities, and challenges, of the digitalising economy."*
>
> **Maggie McGee**
> **Executive Director – Governance, ACCA**

> Public sector procurement is a key feature of government activity in any country and abuse in this area can present significant opportunities for criminals.

Increasing transparency through e-procurement in government

Public sector procurement is a key feature of government activity in any country and abuse in this area can present significant opportunities for criminals. In response to this challenge, Georgia has introduced an e-procurement system that reduces the scope for public sector procurement abuse through the use of digital technology.

The Government of Georgia introduced the new e-procurement system, the Georgia Electronic Government Procurement system, nearly 10 years ago. The system requires full public transparency at every stage of the contracting cycle. It also includes contracts of any value, where many other countries publicly report procurement only above a certain threshold. Bidders are required to participate in any public procurement through the system, reducing the opportunity for bribery and corruption in the public procurement process.

Kakha Demetrashvili, the Deputy Chairman of the State Procurement Agency of Georgia, explained that Georgia has implemented 'one single public procurement electronic system, which is [a] huge portal that is absolutely mandatory for every public procurement case. This includes public–private partnerships and construction projects. Everything in each phase of the public procurement procedures are reflected into the system and we have no monetary threshold for inclusion in the system … in Georgia, all public procurement – irrespective of value – must be included in the e-procurement system, with each stage of the process made publicly available'.

This system has been praised by the United Nations, OECD and Transparency International for improving the governance and checks against public procurement abuse. The Georgia Electronic Government Procurement system provides an example of good practise, where good governance and the effective use of digital technology combine to increase transparency and reduce the scope for public procurement abuse. This example also highlights the potential for governments to use technology in the prevention of economic crime.

Visa applies new technologies to improve the detection and prevention of economic crime

As a major international facilitator of electronic fund transfers, Visa has been at the forefront of applying new technologies to improve the detection and prevention of economic crime.

Jessica Lennard, Senior Director, Global Strategic Data and AI Initiatives, explained that:

Digital economic crime, including fraud, money laundering and cybercrime, is a global, industrialised phenomenon, impacting the lives and livelihoods of all participants in the online economy. This will increase with the growing use of connected devices, such as mobile, tablet, wearables and cards. Continuous investment and an unrelenting focus on the safety and security of the payments network is vital to maintaining consumer trust and protect the ecosystem against this growing risk.

On a fundamental level, the increased traceability and security of digital payments, as opposed to cash, are critical assets in the battle against economic crime. Our 'Cashless Cities' study (Visa, 2019) estimated that greater use of digital payments could reduce money laundering and other cash-related crime by up to 90%.

However, new breakthroughs in advanced technologies, such as machine learning and AI, are expanding the realms of what is possible. Visa has pioneered the use of these technologies in payments for over 15 years, including applying neural network-based AI to real-time transaction risk analysis. The ability to identify and avert fraud in this way has led to historically low levels of less than 0.1%.

Scale and breadth of data facilitates the rapid responses and deep insights required to tackle digital economic crime, for example Visa can process 65,000 transactions a second (approximately 160bn per year). The global nature of the threat also demands a cross-border, co-ordinated approach between industry, law enforcement and regulators. Data flows must not be restricted in such a way as to impede an effective, collaborative response, including safe, secure data sharing. Innovation is also essential and Europe has huge potential in this respect, given the thriving start-up and SME market here.

Any use of AI must, of course, be underpinned by ethical values and practices, and economic crime is no exception. Privacy must be balanced with security, fairness and transparency if consumer trust is to be upheld. ■

> The use of tools such as AI to identify criminal behaviours has an important role to play in fraud detection, but prevention is better than cure, and deterrence should trump detection as a policy outcome to pursue.

Shifting the window – preventing economic crime

The use of tools such as AI to identify criminal behaviours has an important role to play in fraud detection, but prevention is better than cure, and deterrence should trump detection as a policy outcome to pursue. The narrative of using high-profile enforcement actions as a key deterrent is well rehearsed (Stephenson, 2019), and the statistics on regulatory penalties in areas of economic crime are eye-watering (EY, 2018a). Breaches of the US Foreign Corrupt Practices Act (FCPA) frequently attract 8-, 9- and now even10-figure settlements, with individual directors and perpetrators facing significant US jail sentences on prosecution (SEC, 2019).

Use of sanctions as a deterrent is not unique to economic crime, nor a new development directly affected by technology. In fact, statistics tracking enforcement actions under the FCPA and other equivalent legislation do not present a compelling case for their effectiveness as a widespread deterrent. 'Despite over $11bn in fines being issued globally under the FCPA by the US Department of Justice and the SEC [Securities and Exchange Commission], and the UK Serious Fraud Office since 2012, 38% of global executives still believe bribery and corrupt practices remain prevalent in business' (EY, 2018a). Although some time lag is inevitable when measuring behavioural change at an institutional level, the lack of clear correlation between enforcement activity and commission of offences is not encouraging.

We know from research across the fields of criminology, including tax offences and other financial crimes, that criminals regularly underestimate the likelihood of being caught. This has implications for the design of penalty regimes, as the effectiveness of a penalty as a deterrent is unlikely to increase with the magnitude of a sanction if the criminal considers the likelihood of detection and prosecution to be low or nonexistent. High-profile prosecutions are not deterring criminals; instead of thinking, 'I do not want that to happen to me', they think 'that is not going to happen to me'. In the words of Matthew Stephenson, professor of law at Harvard Law School, 'Effective enforcement of anticorruption rules, including criminal law enforcement, against individual wrongdoers is necessary but not sufficient to combat systemic corruption'. (Stephenson, 2019)

Equally, the changing technological landscape could disrupt the effect of countermeasures against economic crime. The usefulness of new detection tools in the corporate environment should be recognised by management, regulators and law enforcement alike and their use encouraged within legal frameworks adapted to give weight to evidence generated and curated by AI tools. Criminals are more likely to refrain from illegal activities if they judge that the risk of detection is too great.

Integrity is key to the organisational 'hostile environment' for economic crime. Building on the core elements of governance, culture, controls and insights, the business can blend human factors with enhanced tools using innovative techniques to bridge the gap between organisational intentions and actions (Gordon, 2019). As the information gathered from enhanced monitoring and analysis in the control environment feeds into a better understanding of the human decisions that characterise the business, so the governance mechanisms can adapt to create and enhance a culture of compliance, in which doing the right thing, and avoiding the opportunity cost of dealing with the aftermath of doing the wrong thing, becomes the default position.

These updated and evolved structures will demand changes in the skills and approaches of employees and management, as well as in policies and processes. Companies will need to invest in their staff so that they will understand the implications of the effective use of AI, and to appreciate the legal and reputational consequences of failure to understand the risks that AI presents. The step change in data management heralds a transformation in compliance departments as ethical values come to the fore. 'Above all, humans need to supervise and control the process. In the age of AI, this is a big ask of a company's senior executives, but this is what is required and demanded of them' (EY, 2019).

A number of the interviewees we consulted pointed to the importance of effective whistle-blowing mechanisms that support both the prevention and detection of economic crime.

One intrinsically human element of the fight against crime is the whistle-blower. A number of the interviewees we consulted pointed to the importance of effective whistle-blowing mechanisms that support both the prevention and detection of economic crime. For example, Harbinson saw the 'development [of] whistle-blowing programmes within your own organisation' as a critical step in the defence against economic crime. He went on to note that this protection must 'be accessible to your suppliers and your customers'.

A series of surveys into the awareness of, and impact on, smaller businesses of bribery and corruption found that respondents ranked high-profile prosecutions as only the fourth most effective option of the five offered, with whistle-blowing laws and mechanisms rising from third place in 2007 and second in 2013 to being ranked the most effective of the options by 2019 (ACCA, 2007; Davies and Mirkovic, 2013a, 2013b; ACCA, 2007, 2019a, 2019b). In the resource-constrained SME sector, access to stakeholder programmes, whether provided by government or supply-chain partners, will be essential. In practice, the challenges of effectively implementing whistle-blower programmes must not be underestimated. Creation of regulation and process is less than half the battle, with cultural factors both in business and society at large often compromising the effectiveness of such initiatives.

THE ROLE OF AUDITING PROFESSIONALS

In addition to the internal controls used by business, the scope for impact on the audit profession should be explored. Survey work by ACCA measuring perceptions among the general public uncovered a widespread belief in respondents that auditors should be responsible for uncovering fraud at every level (notwithstanding materiality considerations and current regulatory frameworks). Globally, just 30% of respondents recognised that there might be some limitations to auditors' ability to detect fraud, while in the UK, 69% of the public respondents expected auditors to detect fraud that would affect financial statements or detect and report all fraud, regardless of size or impact (ACCA, 2019c).

Historically, the response to this from the profession might well have been that, however attractive such an aspiration might be, and regardless of the conceptual role of the auditor, 100% analysis would require such intensive resource deployment as to be economically impossible. But the techniques being used to detect and predict anomalous behaviour in real time could potentially be deployed in a historic audit to uncover patterns apparent only in hindsight. Of course, detecting all economic crime will remain impossible in the face of determined criminals

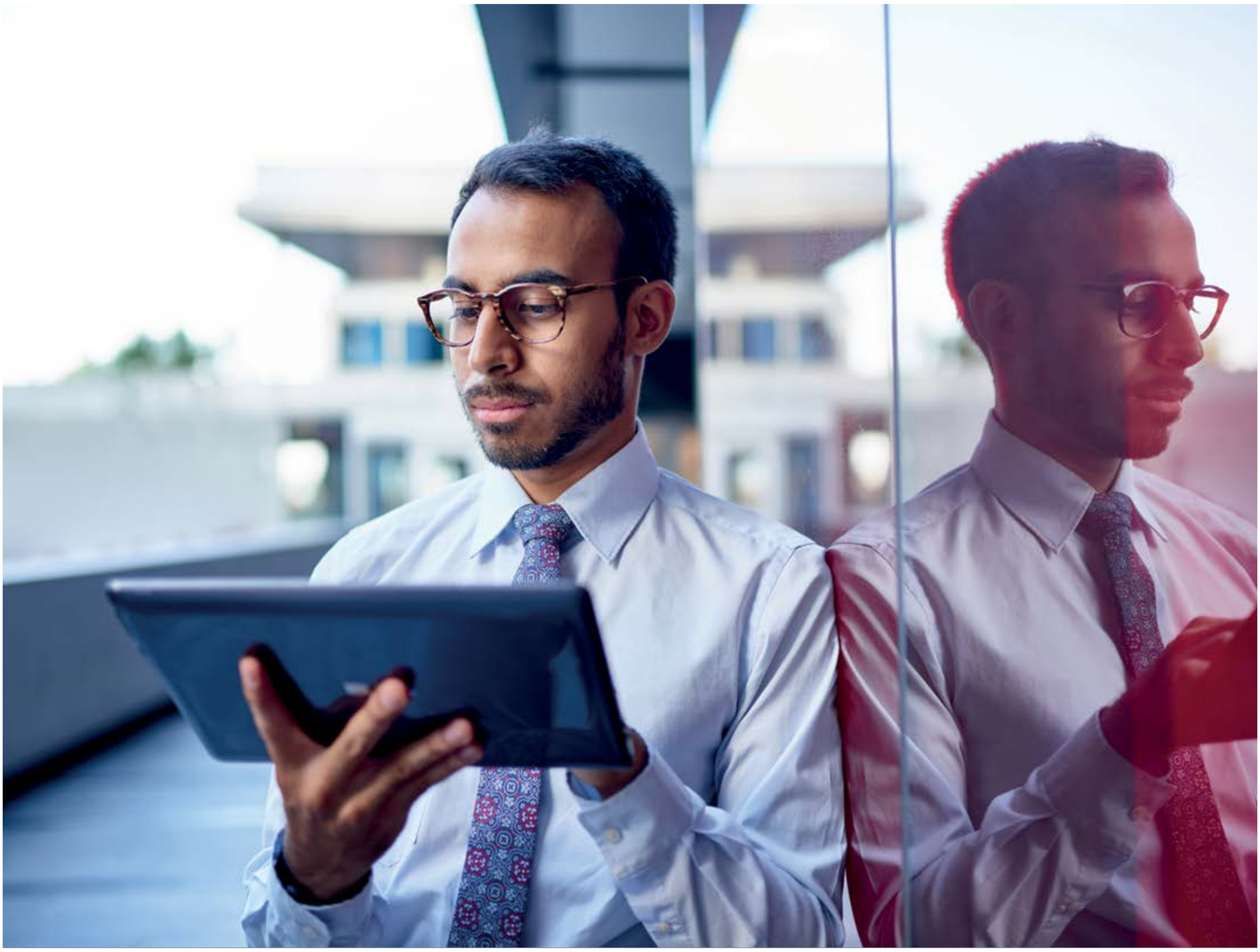
> *"Business technology is no longer an administrative tool; it's fundamental component of the compliance environment, and an integral part of the defences as it becomes a vector of attack. Making the right decisions, at both strategic and tactical levels, will depend on the right talent having the right skills and the right information to tackle the rapidly changing digital world."*
>
> **Mike Suffield**
> **Director – Professional Insights, ACCA**

Ultimately, this integrated and responsive framework of countermeasures and assurance will help to build trust in the ability of business to manage the risks to society posed by digital economic crime.

deploying equivalent technologies to evade detection; but if the cost of hiding the crime outweighs the benefit of committing it, then this alone will act as a deterrent to the rational criminal.

But even with the benefit of analysis for flagging areas of concern, there will still be a role to play for the skilled and sceptical auditor. The effectiveness of these mechanisms relies not just on the effective use of technology, but also on human intervention. 'We should put as much effort into how we train people to use predictions as we do into the predictions', was the conclusion of a Harvard researcher investigating claims of bias in AI-assisted bail decision scoring (Simonite, 2019). The challenge for the audit profession will lie in addressing the skills gap as much as the technology gap.

Professionals must, of course, develop the ability to use new tools to support internal compliance functions by assessing their fraud countermeasures, but to maximise the impact of that work, they will need to interpret and present their findings to management and regulators effectively. Clear and effective communication of the outputs of their assurance work will assist those responsible for fraud detection to develop better systems, and those responsible for developing regulation to implement frameworks and obligations that reflect the capabilities of the new technology. Ultimately, this integrated and responsive framework of countermeasures and assurance will help to build trust in the ability of business to manage the risks to society posed by digital economic crime.



Panel of interviewees

Patrick Craig
Partner and EMEIA Financial Crime Technology Lead, Ernst & Young LLP United Kingdom

Kakha Demetrashvili
Deputy Chairman of the State Procurement Agency of Georgia

Anthony Harbinson
Director Safer Communities, Northern Ireland

David Higginson
Partner, Ernst & Young LLP United Kingdom, Forensic & Integrity Services

Scott Jarrell
Americas Forensic Data Analytics Leader, Ernst & Young LLP United States, Forensic & Integrity Services

Claire Jenkins
Forensic Accountant and UK Tackling Economic Crime Awards' Outstanding Female Professional

Jack Jia
Partner, Ernst & Young – Hong Kong, Forensic & Integrity Services

Nick Maginot
Partner, Ernst & Young – Australia, Forensic & Integrity Services

Anne McCormick
EMEIA Public Policy and Network Engagement Leader, Ernst & Young

Mark Le Page
Director, Ernst & Young LLP United Kingdom, Advisory

Glenn Perachio
Partner and Forensic Technology Leader, Ernst & Young LLP United Kingdom, Forensic & Integrity Services

Rachel Sexton
Partner, Ernst & Young LLP United Kingdom, Forensic & Integrity Services

Narayanan Vaidyanathan
Head of Business Insights, ACCA

REPORT AUTHORS

Jason Piper, Head of Tax and Business Law, ACCA
Jason leads ACCA's policy work on the closely related fields of tax and business law, considering both the direct impacts of developments in each field and the wider implications for business and society as a whole. He has a background in tax practice, and degrees in European and International Commercial Law.

Alex Metcalfe, Head of Public Sector, ACCA
Alex Metcalfe leads on developing thought leadership for the public sector and represents ACCA at a variety of forums. He has worked across central, provincial and local government in the UK and Canadian civil service, including as a senior economist – specialising in tax policy.

References

ACCA (2007), *Bribery and Corruption: The Impact on UK SMEs* <https://www.accaglobal.com/content/dam/acca/global/PDF-technical/small-business/tech-ms-bac.pdf>, accessed 8 September 2019

ACCA (2019a) *Combating bribery in the SME Sector* <https://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/CombatingBribery2019/JasonPiper.CombatingBriberySMEsector.pdf>, accessed 19 November 2019

ACCA (2019b) *Combating bribery in the SME sector – UK analysis* <https://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/CombatingBribery2019/pi-combating-bribery-SME-UK.pdf>, accessed 19 November 2019

ACCA (2019c), *Closing the Expectation Gap in Audit* <https://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/Expectation-gap/pi-closing-expectation-gap-audit.pdf>, accessed 14 November 2019.

AUSTRAC (2019) 'Fintel Alliance' [website article] <https://www.austrac.gov.au/about-us/fintel-alliance>, accessed 14 November 2019.

Chartis and EY (2015), *Tackling Financial Crime through Integrated Risk and Compliance* <https://www.ey.com/Publication/vwLUAssets/ey-tackling-financial-crime-through-integrated-risk-and-compliance/$FILE/ey-tackling-financial-crime-through-integrated-risk-and-compliance.pdf>, accessed 14 November 2019.

Cox, K. (2019), 'NY Regulators Investigating Apple Card after Viral Complaints of Sexism' [website article], 11 November <https://arstechnica.com/tech-policy/2019/11/ny-regulators-investigating-apple-card-after-viral-complaint-of-sexism/?fbclid=IwAR1wN2vY1om6jgqSk1aHdpXV4cf4x9vJO9MSgWp1sJrg-eN83JUp0EikSkU>, accessed 14 November 2019.

Davies, J. and Mirkovic, R. (2013a), *Combating Bribery in the SME Sector: The UK Findings* <https://www.accaglobal.com/content/dam/acca/global/PDF-technical/other-PDFs/tech-tp-cbissuk.pdf>, accessed 6 September 2019.

Davies, J. and Mirkovic, R. (2013b), *Combating Bribery in the SME Sector* <https://www.accaglobal.com/ab44>, accessed 6 September 2019.

Emerging Technology from the arXiv (2019), Bitcoin transactions aren't as anonymous as everyone hoped [online article] *MIT Technology Review* <https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/>, accessed 19 November 2019.

Europol (2019), 'Economic Crime' [website article] <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime>, accessed 14 November 2019.

EY (2016), *If an Employee Goes Rogue, How Will You Know?* <https://www.ey.com/Publication/vwLUAssets/ey-if-an-employee-goes-rogue-how-will-you-know/$FILE/ey-if-an-employee-goes-rogue-how-will-you-know.pdf>, accessed 14 November 2019.

EY (2018a), *Integrity in the Spotlight: The Future of Compliance: 15th Global Fraud Survey* <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-integrity-in-spotlight.pdf>, accessed 14 November 2019.

EY (2018b), *How can you disrupt risk in an era of digital transformation? Global Forensic Analytics Survey 2018* <https://www.eycom.ch/en/Publications/20181203-Global-Forensic-Data-Analytics-Survey-2018/download>, accessed 15 November 2019.

EY (2019), *Is your algorithm an ethical one?* <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-is-your-algorithm-an-ethical-one.pdf>, accessed 14 November 2019.

EY (n.d.a.), 'Disrupting financial crime' [website article] <https://www.ey.com/en_gl/disrupting-financial-crime>, accessed 14 November 2019.

Fintech Times (2019) UK Public Overwhelmingly Unaware of Deepfake Threat [website article] <https://thefintechtimes.com/deepfake-threat/> accessed 19 November 2019.

Fraud Advisory Panel (2018), *Fraud Futures: Understanding the Old to Prepare for the New* <https://www.fraudadvisorypanel.org/wp-content/uploads/2018/06/Fraud-Futures-WEB-July-2018.pdf>, accessed 14 November 2019.

Gartner (2019a), 'Gartner Glossary: Artificial Intelligence (ai)' [website article] <https://www.gartner.com/en/information-technology/glossary/artificial-intelligence>, accessed 14 November 2019.

Gartner (2019b), 'Gartner Glossary: Robotic Process Automation (rpa)' [website article] <https://www.gartner.com/en/information-technology/glossary/robotic-process-automation-rpa>, accessed 14 November 2019.

Gordon, A. (2019), 'How to Drive the Future of Compliance with Integrity in the Spotlight' [website article], 10 June <https://www.ey.com/en_gl/assurance/how-to-drive-the-future-of-compliance-with-integrity-in-the-spotlight>, accessed 14 November 2019.

Gov.uk (n.d.), Centre for Data Ethics and Innovation' [website] <https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation#content>, accessed 14 November 2019.

Jones, T. (2018), 'Genoa's tragedy points to a malaise at Italy's heart' [online article], *The Guardian*, 19 August <https://www.theguardian.com/commentisfree/2018/aug/19/genoa-bridge-tragedy-points-to-malaise-italy-heart>, accessed 19 October 2019.

Matthew (2018), 'German Government Accuses Lufthansa of Illicit Price Hikes' [website article], 4 January <https://liveandletsfly.boardingarea.com/2018/01/04/lufthansa-price-fixing/>, accessed 14 November 2019.

Refinitiv (2018), *Revealing the Cost of Financial Crime: 2018 Survey Report* <https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/true-cost-of-financial-crime-global-focus.pdf>, accessed 14 November 2019.

SEC (US Securities and Exchange Commission) (2019), 'SEC Enforcement Actions: FCPA Cases' <https://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml>, accessed 1 December 2019.

Simonite, T. (2019), 'Algorithms Should've Made Courts More Fair. What Went Wrong?' [online article], *Wired* <https://www.wired.com/story/algorithms-shouldve-made-courts-more-fair-what-went-wrong/>, accessed 14 November 2019.

Stephenson, M. (2019), 'Aggressive Criminal Law Enforcement is Insufficient to Combat Systemic Corruption. But that Doesn't Mean it's not Necessary', [website article], *GAB: The Global Anticorruption Blog*, 19 November <https://globalanticorruptionblog.com/2019/11/19/aggressive-criminal-law-enforcement-is-insufficient-to-combat-systemic-corruption-but-that-doesnt-mean-its-not-necessary/>, accessed 1 December 2019.

Sullivan, T. (2018), '3 Charts Show where Artificial Intelligence is Making an Impact in Healthcare Right Now' [online article], Healthcare IT News, 21 December <https://www.healthcareitnews.com/news/3-charts-show-where-artificial-intelligence-making-impact-healthcare-right-now>, accessed 14 November 2019.

Transparency International (2017), 'Global Corruption Barometer: Citizens' Voices from around the World' [website article], 14 and 15 November <https://www.transparency.org/news/feature/global_corruption_barometer_citizens_voices_from_around_the_world>, accessed 4 September 2019.

Waters, R. (2016a), 'Automated Company Raises the Equivalent of $120 million in Digital Currency' [online article], *Financial Times*, 16 May <https://www.ft.com/content/600e137a-1ba6-11e6-b286-cddde55ca122>, accessed 13 November 2019.

Waters, R. (2016b), '"Ether" Brought to Earth by Theft of $50m in Cryptocurrency' [online article], *Financial Times*, 16 June <https://www.ft.com/content/591518a0-34df-11e6-ad39-3fee5ffe5b5b>, accessed 13 November 2019.

PI-ECONOMIC-CRIME-DIGITAL-AGE

EYG NO. 005752-19GBL

ACCA The Adelphi 1/11 John Adam Street London WC2N 6AU United Kingdom / +44 (0)20 7059 5000 / www.accaglobal.com