The potential impacts of the digital revolution on the operational risk profiles of banks

Received (in revised form): 24th October, 2023

Michael Grimwade
Managing Director, Operational Risk, ICBC Standard Bank, UK

Michael Grimwade first worked in operational risk management almost 30 years ago. He is Head of Operational Risk for ICBC Standard Bank and has previously held senior operational risk management roles at MUFG Securities, Royal Bank of Scotland and Lloyds TSB, and he has also been a director of the Institute of Operational Risk. Michael is the author of a number of papers on quantifying emerging risks, modelling operational risk capital and climate change, and he received an award in 2014 from the Institute of Operational Risk for his contribution to the profession. His second book, 'Ten Laws of Operational Risk' was published in December 2021.

Operational Risk, ICBC Standard Bank Plc, 20 Gresham Street, London EC2V 7JE, UK
E-mail: michael_s_grimwade@yahoo.co.uk

Abstract Society is undergoing a digital revolution. This is altering the business profiles of banks in terms of their systems, processes, controls and usage of third parties; their competitive landscape, ie competition from both digitising incumbents and new BigTech and FinTech entrants; and the behaviours of stakeholders, ranging from customers to cyber-criminals. This digital revolution is amplifying some of their existing risks, while also creating new risks, eg the potential for artificial intelligence (AI) tools to change behaviours over time (AI model drift). Some of these changes in operational risk profile will be transient, as they are associated with digital transformation, while others will be both ongoing and characterised by a high degree of dynamism. In this digitised endstate higher frequency/lower value human errors, may be replaced by lower frequency/higher impact systemic losses, arising from both catastrophic and silent failures.
The influence of the digital revolution spans almost all of the Basel operational risk event categories, and may also lead to the enhancement of some controls (eg surveillance), while others may be undermined (eg by voice-spoofing). There is no silver bullet to mitigate these risks; instead, a portfolio of existing control frameworks need to be enhanced, including the following: change management; model risk management; third party vendor management; business continuity management, disaster recovery and operational resilience; and cybersecurity, with new controls required to address the new risks associated with AI. This will be a key factor in the operational risk losses of banks over the next decade.

Keywords: *digital revolution, digitisation, artificial intelligence, AI, BigTech, FinTech, operational risk*

INTRODUCTION

Society is undergoing a digital revolution which is altering the business profiles of banks, their competitive environments and the behaviours of their stakeholders. This digital revolution is enabled by a series of technological advances, such as the development of the Internet, smart phones and artificial intelligence (AI), that are underpinned by faster, cheaper and bigger processing and storage capabilities. Almost all aspects of banking are changing in response to technology-enabled competition from both incumbents and new entrants: the greater willingness of customers to use a portfolio of financial service providers and shareholder pressures to improve returns. The Organisation for Economic Co-operation and

Development (OECD) observed that 'Banking is undergoing a transformation from being based in physical branches to using IT and big data' and that this digital revolution has 'greatly increased the weight of codified information and the tools that are available to process it, Artificial Intelligence (AI) [. . .] using big data'.[1]

This paper is focused on the consequences of this digital revolution on the operational risk profiles of banks, and is organised into the following four sections:

1. Why and how banking is being transformed by the digital revolution.
2. How the digital revolution may alter the operational risk profiles of banks:
   - digital transformation;
   - AI;
   - third and fourth party suppliers;
   - controls — both AI enhancements and degradations;
   - criminal innovation.
3. What actions should operational risk managers be taking to mitigate these risks.
4. Conclusions.

As the risks of the digital revolution are still emerging, the examples in this paper are taken from a wide variety of industries, not just financial services, to illustrate potential consequences.

WHY AND HOW BANKING IS BEING TRANSFORMED BY THE DIGITAL REVOLUTION

Over the course of the author's career, the business profile of retail banking has moved from branches, which sold products and services and processed cash, cheques and customer requests between the hours of 9 am and 3 pm, five days a week, to online, 24/7 banking, in which payments are increasingly digital and nearly instantaneous. In the UK, this has contributed to more than half of the bank branches that existed in the mid-1980s being closed. In 1986 there were ~21,600 bank and building society branches in the UK, but by 2022 there were just ~8,000.[2] The COVID-19 pandemic may have accelerated this existing trend, for instance in the UK cash payments represented ~23 per cent of all payments in 2019, but this had declined to just ~15 per cent by 2021.[3] Similarly, investment banking has moved from open outcry and phone trading to increasingly electronic and algorithm-driven trading, with the last open outcry pits on the London International Financial Futures and Options Exchange (LIFFE) trading floor closing in November 2000.

The breadth of the impacts of this digital revolution on banking is illustrated in Figure 1, which represents both the internal infrastructure of banks and the key stakeholders with which they interact.

The remainder of this section illustrates the nature of the digital revolution in terms of three of the components in Figure 1, ie BigTech and FinTechs, customers and clients, and the firms themselves.

BigTechs and FinTechs

In addition to providing technology services to banks, such as infrastructure (IaaS) and software-as-a-service (SaaS), BigTechs may also act as both competitors and partners with banks by providing basic financial services to their large networks of customers, and by acting as distribution channels for third party product providers. Payment services have historically been one of the first financial services offered by BigTech. Their offerings can be split into two categories:

1. Payments in emerging economies may involve the introduction of new entities and operations outside of traditional financial and banking networks. For example, Vodafone's and Safaricom's M-PESA payment service in East Africa utilises the mobile phone network.
2. In more developed markets, BigTechs' payment services are overlaid on existing banking services, such as credit and debit cards, eg Apple Pay and PayPal.

BigTechs' inroads into payments have been greatest where the existing provision of payment services is limited and mobile phone penetration is high.[4,5] In the EU, the second Payment Services

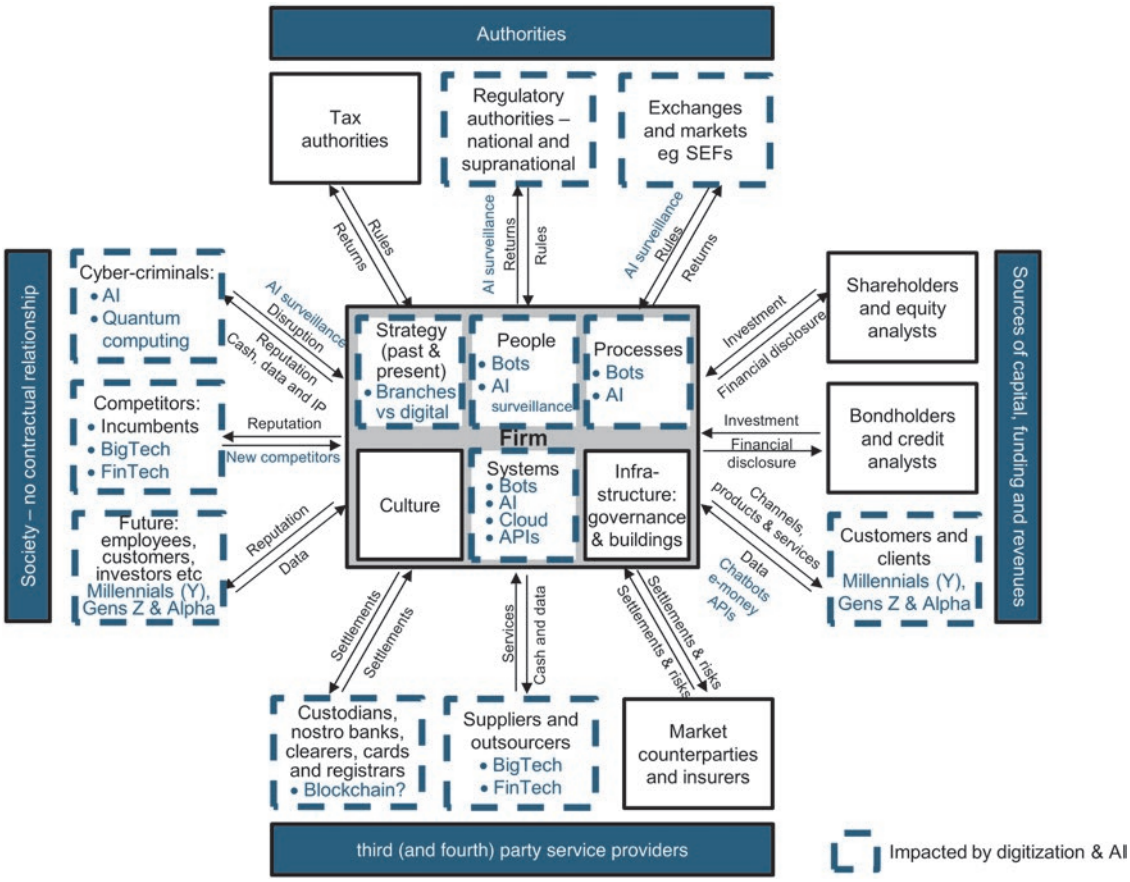

Figure 1: The changing business profile of banks due to digitisation

Directive (2018) has led to a growth in BigTech firms with licensed payment subsidiaries.[6]

BigTechs can also leverage their customer bases to offer money market funds and insurance products via their platforms. Money market funds can be linked to their payment services, ie surplus account balances can be invested in money market funds. This primarily occurs in China, for example Alipay, but even in China the value of the BigTech funds are a fraction of bank deposits. These money market funds and insurance products may be provided by BigTech affiliates or by third party providers.

While some BigTechs have begun to lend (mainly to small and medium-sized enterprises and consumers with short maturities) the expansion into lending has been strongest in those jurisdictions with lighter financial regulation and higher banking sector concentration. Although the access of BigTech to customer data, combined with machine learning, may give them a competitive advantage in predicting default, BigTech lending is ultimately limited by their inability to take retail deposits without obtaining banking licences. Obviously this is not an issue for FinTech peer-to-peer lending platforms, as these allow individuals and companies to lend directly to borrowers, either individually or to packages of loans, without bank intermediation. Examples included LendingClub (US) and Funding Circle (UK), but in recent years both have exited from peer-to-peer lending.

BigTech incursions into financial services regarding payments — and to a lesser extent, lending — as well as the *bundling* of other bank services may squeeze bank profitability, driving the need for efficiency improvements through new technology. In contrast, FinTechs may similarly impact bank profitability but by *unbundling*

individual services traditionally provided by banks, capitalising on an environment in which their customers are increasingly willing to embrace both new technologies and new service providers (as discussed in the next section).

Customers: Changing behaviours

Surveys of customers have found that younger generations (eg millennials and Generation Z [Gen Z]) are less satisfied with their incumbent banks than older generations (eg baby boomers).[7] While all generations have shown a willingness to embrace new technologies and service providers such as FinTechs, the younger generations have a greater tendency to utilise multiple FinTech service providers.[8] This is particularly important as millennials and Gen Z now represent the largest generational demographics in the US, and millennials are currently the largest driver of new net loans, although this will soon pass to Gen Z.[9]

Banks: Improving efficiency and controls

For banks the digital revolution may variously deliver operational efficiencies through greater automation, enhancements to controls and improved data-based decision making.

Operational efficiencies may arise from the automation of low value, repetitive activities, for example, through the use of automated computer programs or *bots* for activities such as responding to audit letters or correcting errors in fund transfer requests, but at the potential expense of architectural complexity. One example is the introduction by JPMorgan Chase of its COiN (contract intelligence) platform, which uses machine learning to analyse legal documents in order to extract important data.[10] Chatbots now commonly interact with customers to solve simple problems, with machine learning facilitating the identification of customer requirements and, if necessary, transferring customers to human agents. Chatbots may increasingly be used to provide internal help-desk services to staff. In addition, cloud computing may provide banks with processing and storage capabilities that are potentially lower in cost and more flexible.

Enhancements to controls include the harnessing of machine learning to identify suspicious activities (eg anti-money laundering [AML] and fraud detection) and to flag potential cases for review by bank staff. In the future, the current compliance surveillance of traders' communications — using multi-lingual lexicons of key words — may be replaced by AI that intelligently understands the meaning of language.

Credit approvals for retail customers have long been automated and based on scorecards, while on trading floors, it is beginning to be employed to evaluate venue, timing and order size choices to optimise the filling of orders.

Conclusions

The drivers of this digital revolution seem unstoppable. Technological advances continue apace, and they are being increasingly embraced by customers. Banks that harness these technologies will reap the benefits of operational efficiencies through greater automation, enhancements to controls and improved data-based decision making. Banks that do not embrace these changes are at risk of suffering customer and revenue attrition due to competition from digitised incumbents and new BigTech and FinTech entrants, leading to poorer returns than their digitising peers. Digitisation, however, will clearly alter the operational risk profiles of firms, both during the transition and permanently in the new end-state. This is explored further in the next section.

HOW THE DIGITAL REVOLUTION MAY ALTER THE OPERATIONAL RISK PROFILES OF BANKS

The digital revolution is changing the risk profiles of firms by creating new operational risks as well as amplifying existing risks, ie by making failures potentially more systematic, creating concentrations of data, introducing new single points of failure and fuelling criminal innovation. As noted above, some of these changes in the operational risk profile will be transient, restricted to the duration of a firm's migration to a more digitised business model, while other changes will be permanent.

Table 1 sets out an extract of the Basel II event taxonomy and highlights that six of the Level 1 risks may variously be influenced by five different aspects of the digital revolution, which are causal factors. These are illustrated by examples from a range of industries as well as rules-based and AI-powered algorithms. The remainder of this section considers these five causal factors in more detail:

- digital transformation;
- AI;
- third and fourth party suppliers;
- controls, both AI enhancements and degradation;
- criminal innovation.

Digital transformation

As stated by the OECD, 'In order to achieve improved efficiency, the incumbents must restructure simultaneously with the entry of new competitors'.[11] The execution of digital transformation may lead to five potential points of operational failure (Figure 2):

1. *Stresses on business as usual (BAU) activities*, caused by the redirection of resources to a firm's overall digital transformation programme, leading to increased operational risk losses. The resources being redirected may include both experienced staff members and technology resources needed to provide fixes and enhancements to BAU processes and legacy applications.
2. *Uncovering latent issues*. The process of digitising and migrating data may uncover historical operational failures which have remained latent for extended periods of time, eg misbookings or deficiencies and/or omissions in legal documentation; digital transformation may accelerate the identification of these previously hidden issues. The decommissioning of legacy infrastructure may also uncover latent issues as well as functionality that has silently accreted over time. Finally, the automation of processes that results in headcount reductions may act as a trigger for staff litigation.
3. *Risks of migration/transition to the next state*. This includes a range of operational failures including those associated with data quality and data leaks, the functionality and performance of AI, and systems integration. The disruption suffered by TSB in 2018 is illustrative of the potential risks of migration during strategic transformation programmes.
4. *Weaknesses associated with any interim-states*. While phasing transformation programmes helps to mitigate the risks of migration, new potential risks may arise from running strategic digitised and legacy systems and processes in parallel. This can lead to issues from gaps or overlaps in transactional data and inconsistencies in reference data and conventions, eg the treatment of public holidays or end of day cut-off times etc. Additionally, as customers may increasingly interact with their banks regarding a single complex transaction via multiple channels, eg online, chatbots and call centres, then banks must be able to integrate these information flows between the different channels in any interim-state, as well as in the eventual end-state.
5. *Weaknesses in the end-state*. The strategic digitised architecture may integrate applications with bots, AI, APIs and partnerships with FinTechs, all of which may run in the cloud. This end-state may act as 'an amplifier of existing'[14] risks, eg transforming the high frequency/low value human errors into much lower frequency, but much higher severity risks of systemic technology failures. It may also introduce new risks and vulnerabilities, for example new single points of failure in the form of the cloud and third parties, data privacy issues, a blizzard of AI generated false positives, silent failures over time through AI model drift (eg discriminatory lending), unintended native functionality in third party software and the potential to exclude less technologically sophisticated customers.

While none of these risks associated with change are clearly unique to digital transformation, the potential scale of change and volume of data involved makes them more significant.

The remainder of this section considers the risks associated with the digitised end-state in more detail.

Table 1: The digital revolution: analysis of how operational risks may be influenced by the five causal factors

Basel II, levels		Level 3 Examples of IT and cyber operational risks, ie the risk of loss arising from . . .	Digital transformation	AI	Third and fourth parties	Controls	Cyber-criminals
1	2		Transient	Ongoing and dynamic			
BDSF	Systems	• Disruption of software, both accidental or malicious, eg TSB's botched systems migrations (2018).	x	x	x		x
		• Disruption of data and storage, both accidental or malicious.	x		x		x
		• Hardware failures, both accidental or malicious, eg Stuxnet virus disrupts Siemen centrifuges (~2007).	x				x
		• Disruption of own infrastructure, both accidental or malicious, eg RBS's batch-scheduler issues (2012).			x		x
		• Disruption of external infrastructure, both accidental or malicious.			x		x
		• Disruption of vendors and suppliers of IT services, both accidental or malicious, eg SunGard UK's administration (2022) or the ransomware attack on Ion (2023).			x		x
EDPM	Transaction capture, execution and maintenance	Various malfunctions, eg: • System miscalculations. • Incorrect decisions, eg a blizzard of false positives. • System generated duplicated or erroneous transactions.	Caused by, for example: • *Data issues,* eg quality, completeness, biases etc; or • *Model issues,* eg design, model drift etc.	x x x		✓ ✓ ✓	
CPBP	Suitability, disclosure and fiduciary	• Breach of privacy — errors.		x	x		
		• Breach of privacy — exceeds legal authority, eg Facebook's EUR1.2bn fine (2023).	x	x	x		
		• Breach of contract/intellectual property rights through utilising the outputs of ChatGPT.	x	x			
		• Inappropriate advice, eg robo-advice litigation in Hong Kong (2019).		x	x	✓	
	Improper business practices	• Automation of improper trade/market practices, eg abuse of last-look (2015) and *Dr Evil* (2004).		x		✓	
		• Automation of improper trade/market practices from AI, eg discriminatory lending		x		✓	
		• Exploitation of AI through deliberate manipulation by sophisticated third parties, eg chatbot Tay (2016).		x		✓	x
		• Exclusion of less technologically sophisticated customers.	x	x			

Table 1: The digital revolution: analysis of how operational risks may be influenced by the five causal factors (continued)

Basel II, levels		Level 3 Examples of IT and cyber operational risks, ie the risk of loss arising from . . .	Digital transformation	AI	Third and fourth parties	Controls	Cyber-criminals
1	2		Transient	Ongoing and dynamic			
EF	Theft and fraud	• Cyber theft of firm's cash or cryptocurrency, eg Bangladesh Bank theft (2016).				x	x
		• Cyber theft of clients' cash or cryptocurrency from firm, eg cryptocurrency theft from BitMart (2021).				x	x
		• Cyber investment frauds, eg by establishing a clone of a bank's website — these are very numerous.				✓/x	x
		• Application fraud, eg using phished data or scraped from the internet by AI.				✓/x	x
	Systems security	• Cyber theft of client data from banks, eg the JPMorgan Chase data theft (2014).				x	x
		• Cyber theft of data from banks' suppliers and vendors, eg the Equifax data theft (2017).			x	x	x
		• Cyber theft of bank customers' data from unrelated third parties, eg the eBay data theft (2014).			x	x	x
		• Cyber theft of intellectual property, eg AI model code.				x	x
		• Cyber extortion from banks, eg CajaGlobal (2023).				x	x
IF	Unauthorised activity	• Malicious breach of privacy, eg uploading intellectual property into ChatGPT, Samsung (2023).		x			
		• Malicious destruction of assets.					
	Theft and fraud	• Theft of intellectual property, eg computer code for AI. Previous thefts have related to HFT code.		x			
		• Theft of client data.	x				
		• Procurement frauds by technology staff.			x		
EPWS	Employee relations	• Employee litigation, eg changing roles or redundancy resulting from the digital revolution.	x				
		• Unsuccessful candidates, eg Amazon's reportedly discriminatory machine learning powered CV screening tool (2014).		x			

While the Level 1 and 2 risks reflect Basel II's risk taxonomy, the Level 3 risks are based on an analysis of ~900 IT and cyber operational risk events.[12]

x, increased risk; ✓/x, both enhancing controls, but also degrading controls ✓ enhancing controls.

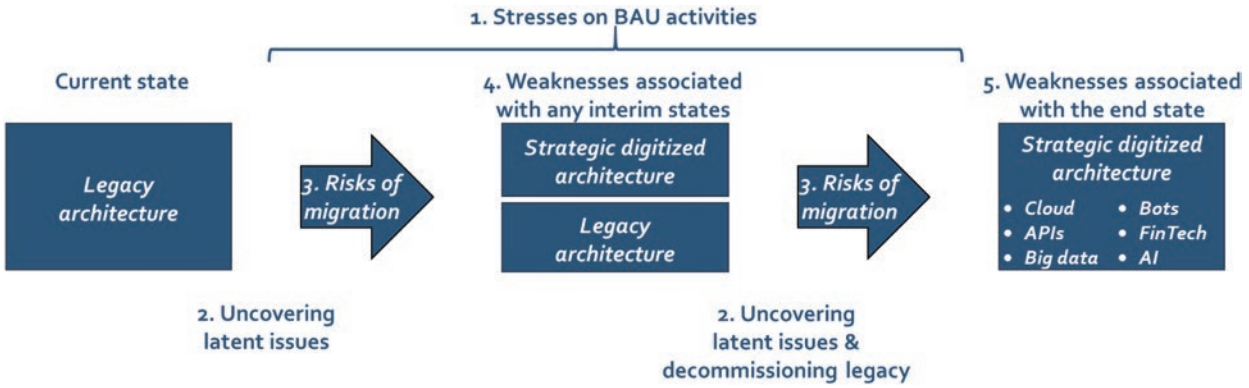

Figure 2: The operational risk profile of digital transformation[13]

AI

As Table 1 illustrates, there are a wide range of risks that are influenced by AI and big data, including:

- *data issues*: the malfunctioning of AI as a consequence of data issues, eg errors in training data, incomplete or unrepresentative data, historical data biases, insufficient data, poor data validation, etc;[15]
- *model issues*: the malfunctioning of AI as a consequence of model issues, eg inappropriate model choices, errors in model design or construction, unexpected behaviours or consequences, AI model drift, etc;[16]
- *inappropriate usage of AI*, eg to commit market abuse;
- *exploitation of AI*, eg again to commit market abuse;
- *data leakage and data privacy issues*; and
- *intellectual property infringements*.

AI malfunctions: Data issues

The quality of data used to train AI is crucial to its intended operation. This is illustrated by a widely reported issue relating to a machine learning tool, developed by Amazon in 2014, to review job applicants' CVs. The model was trained to assess applications by studying CVs submitted to Amazon over a 10 year period, which, *reportedly*, led it to learn to favour male candidates for software developer jobs and other technical posts and to downgrade applicants whose CVs contained words such as 'women's' or who were graduates of two all-women's colleges. In 2015, *reportedly* Amazon recognised that the tool was not evaluating applicants in a gender-neutral way.[17] Similarly, in 2019, the National Institute of Standards and Technology (NIST) found widespread evidence of racial bias in 189 facial recognition algorithms as there were higher rates of false positives for Asian and African American faces relative to images of Caucasians. A notable exception, however, was that for some algorithms developed in Asian countries there was no such bias, potentially reflecting the relationship between an algorithm's performance and the data used to train it.[18] In banking, comparable issues may introduce bias into credit scoring tools, which may result in discriminatory lending decisions.

AI malfunctions: Model issues

AI models are clearly not infallible, for example there are reported instances of them hallucinating facts such as the case of an Australian mayor who threatened to sue OpenAI if it did not correct ChatGPT's false claim that he had served time in prison for bribery.[19] While there seem to be no examples (so far) of AI leading to catastrophic failures and operational risk losses for financial institutions, there are examples of losses arising from malfunctioning rules-based trading algorithms, most notably Knight Capital's US$460m loss which it suffered in just 45 minutes in 2012. There was a spate of these events from 2010, after which there have been no material losses, reflecting

improvements in controls and increased regulation, eg Markets in Financial Instruments Directive (MiFID) II's Regulatory Technical Standard-6. These losses may be illustrative of the potential consequences of AI model drift, as the performance of an AI tool may diverge from its original specification over time.

Malfunctioning rules-based algorithms have also been responsible for silent failures over extended periods, for example in 2006 when the Royal Bank Of Canada (RBC) repaid CAD7.2m to 23,000 residential mortgage customers after discovering two errors relating to the calculation of mortgage repayment charges, including a mismatch between RBC's system and the stated terms between 1999 and 2004. Similar losses could arise from AI model drift. A case was also brought in Hong Kong in 2019 by an investor against a hedge fund manager for US$23m of losses that were claimed to have been caused by an AI-powered investment tool, but the outcome of this litigation, at the time of writing, is unclear.[20]

AI: Inappropriate usage

There is the potential for AI to be used to enable staff members and/or firms to act inappropriately in a much more efficient manner. While there are no current examples relating to AI, there are examples of rules-based algorithms being used in this way. For example, the New York Department of Financial Services (DFS) fined Barclays US$150m in 2015 for allegedly implementing 'last look'[21] in an asymmetrical fashion between 2009 and 2014 on its BARX trading platform, ie FX trades that moved in a customer's favour, above a threshold, were rejected by BARX, but not if they had moved in Barclay's favour.[22] Similarly, in 2004, Citigroup leveraged automation to execute its *Dr Evil* trading strategy. This involved building up and rapidly exiting a very large long position in European government bonds, the equivalent of an average day's trading volume, in just 18 seconds on the MTS platform. Citigroup was fined by the FSA for failing to consider the impact of their trading strategy on the market.[23] In the future, misconduct may also be perpetrated by AI: without guardrails (see section below), an AI may single-mindedly pursue its goal but, in the process, do something that is harmful to markets and/or customers that was not the desired outcome. This is the financial services' equivalent of the AI-run paperclip factory thought experiment.[24]

AI: Exploitation

The behaviours of AI can be maliciously exploited by third parties. For example, on 24th March, 2016, Microsoft launched a chatbot — Tay — that was designed to have conversations with Twitter users and to learn how to mimic humans by copying their speech patterns. Unfortunately, it quickly learned to repeat anti-Semitic and other hateful language that human Twitter users fed the program, forcing Microsoft to shut Tay down just 16 hours after its launch. Microsoft posted a statement saying:

> The AI chatbot Tay is a machine learning project, designed for human engagement. As it learns, some of its responses are inappropriate and indicative of the types of interactions some people are having with it. We're making some adjustments to Tay.[25]

While there are no current examples of trading AIs being exploited, there have been examples of rules-based trading algorithms being manipulated by human traders. For example, in 2015 the Financial Conduct Authority (FCA) fined a former Bank of America Merrill Lynch bond trader for market abuse. Knowing that other market participants often used algorithms to update their quotes by tracking the best bid and best offer on BrokerTec, he entered a series of quotes for low trade sizes, which became the best bids, and waited for the algorithms to raise their quotes in response. He then sold to these other banks, generating a profit, before cancelling his own quotes.[26]

AI: Data leakage and data privacy issues

There are a range of risks associated with ChatGPT regarding both data leakage and data privacy. Uploading proprietary data into AI such as ChatGPT may mean that it is used to provide future public responses. For example, it was reported in April 2023 that Samsung software engineers had sent lines of confidential code to ChatGPT on two separate occasions in order to fix bugs.[27] As a

consequence, it was reported that a number of Korean companies were putting in place guidelines, training and restrictions to prevent recurrence.[28] There are also potential issues associated with AI in terms of data privacy, for example on 4th April, 2023, the Italian data protection authority (Garante) issued a temporary ban to OpenAI regarding ChatGPT due to it being originally trained on personal data. The regulator had concerns over the lack of a legal basis for the use of the personal data, as well as issues over its accuracy.[29]

AI: Intellectual property infringements

Finally, AI that is trained on large quantities of text data, including books and articles, may potentially infringe on the copyright of these works.[30] For example, Getty Images filed a lawsuit in February 2023 in a Delaware court against Stability AI Inc., accusing it of misusing 12 million Getty photographs to train its Stable Diffusion AI image generation system.[31]

Third and fourth party suppliers

The increased usage of third parties as part of digitisation, such as BigTech, can alter the operational risk profiles of firms through both disruption of software and/or infrastructure and data associated issues. The Financial Stability Board has highlighted that BigTech could potentially affect financial stability in several ways:[32]

1. Risks may be magnified by their interlinkages with regulated financial entities, such as partnerships to originate and distribute financial products; and
2. They may also generate risks as they carry out systemically important activities, that are ancillary to financial services, such as, both infrastructure-as-a-service, eg cloud services[33] and also software-as-a-service, as evidenced by the disruption caused by the ransomware attack on Ion in February 2023, or the potential for disruption caused by SunGard UK, a datacentre operator, entering administration in March 2022.

In addition to these systemic risks, there are also third and fourth party risks associated with the loss of data, either through accidents and/or malicious acts, as well as the breach of data privacy rules, such as restrictions on the cross-border movement of data (eg Facebook's 2023 EUR1.2bn fine for storage of personal data outside of the EU),[34] the continued storage and usage of data. Finally, connectivity with providers of SaaS may create contagion risks. Banks may be vulnerable to attack or infection via these links through the introduction of code compromised by malware, such as in the SolarWinds cyber-attack in 2020.

Controls: Both AI enhancements and degradation

AI and machine learning can be used in a variety of ways to improve the effectiveness of controls, but equally these new technologies may be harnessed by cyber-criminals to exploit victims more effectively and efficiently.

Applications of AI to improve control include the prevention and/or detection of frauds, money laundering, market misconduct and rogue trading. Firms can use AI to identify suspicious activities and flag potential cases for review by bank staff. AI could be trained using internal data such as historical data preceding the discovery of fraud or the identification of suspicious activity (eg by using suspicious activity report [SAR] data). This may eventually lead to a rather dystopian future in which AI-powered trading algorithms may themselves be subject to monitoring by AI-powered surveillance tools. There is also the potential, as noted earlier, for existing surveillance of communications based on multi-lingual lexicons of key words to be replaced by AI that understands language.

Other uses of AI to enhance controls may include the following.

- *Identification of lessons learned*: AI could interrogate operational risk data held in governance, risk and compliance (GRC) systems, such as, incidents, key risk indicators (KRIs) and risk and control self-assessments (RCSAs), in order to gain new insights.
- *Automation of data collection*: Some elements of the know your customer data collection could be undertaken by AI through scraping the Internet, although this could lead to data privacy issues.

- *Generative AI*, embedded within a GRC system, may become capable of drafting tailored e-mails in response to incidents, red KRIs and overdue actions etc.
- *Information extractors*: AI could also be used to extract requirements from regulations and then to map them to existing controls.

Unfortunately, as flagged in Table 1, AI does not exclusively provide benefits to the effectiveness of controls as criminals may also utilise these technologies for circumventing existing bank controls. AI-based software now exists that can replicate/spoof voices. For example, in 2019 criminals reportedly used this technology to impersonate the voice of the CEO of a German company in three calls to its UK subsidiary to make a fraudulent, urgent transfer of EUR220k allegedly to an Hungarian supplier, according to the victim's insurers Euler Hermes Group.[35] The UK CEO reportedly recognised his boss' slight German accent and the melody of his voice on the phone. It is unclear whether the attackers also used bots to react to the victim's questions. Obviously this technology has the potential to undermine the integrity of voice recognition software used by some telephone banks.

Similarly the development of quantum computing has created the potential to undermine existing encryption protocols[36] — 'Encryptogeddon'. By the 2030s, practical quantum computing solutions could impact computing strategies across industries', which means that cyber-criminals may pre-empt these developments by employing tactics of 'harvest now, decrypt later'.[37] The World Economic Forum's Future Council on Quantum Computing estimates that ~20 billion digital devices will need to be upgraded or replaced with post-quantum cryptography in the next 20 years.[38] This is reminiscent of the Y2K issue at the end of the last millennium.

Criminal innovation

Professional criminals are rationale, seeking to maximise their returns, and will therefore optimise, like foraging animals,[39] the effort to locate victims, the effort to exploit victims, and the financial rewards obtained. Consequently, any changes in customer and/or bank behaviours (effort to locate), usage of technology by both banks and criminals (effort to exploit), or concentrations of data through digitisation (financial rewards) will lead to predictable changes in criminal behaviours. For example, text generating AI may prove to be both more efficient and effective at phishing, social engineering, encouraging people to click on links infected with malware, or to make fraudulent *urgent* payments in response to messages purporting to come from their relatives, friends or colleagues. This will effectively amplify existing cyber-crime risks.

As the world has digitised, there has been an increase in the occurrence of data hacks, and since 2014, there have been a series of very significant data losses involving more than 500 million records (Figure 3). The targets are often social media (eg Facebook and LinkedIn), technology (eg Yahoo and SolarWinds), retail (eg eBay), outsource service providers (eg Equifax) or governments, because 'that's where the data is'.[40] While only one of the firms in Figure 3 is a global systemically important bank (G-SIB), JPMorgan Chase (reflecting a

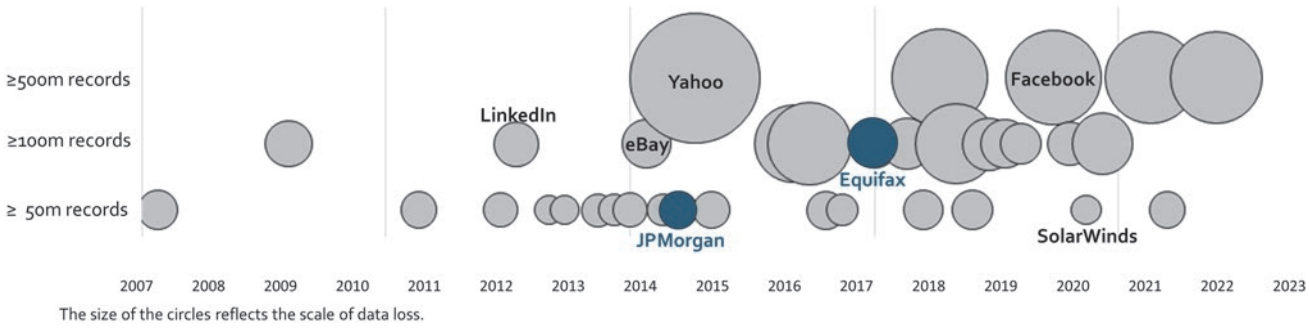

Figure 3: Distribution of data thefts of more than 50 million records in the public domain over the last 15 years[41]

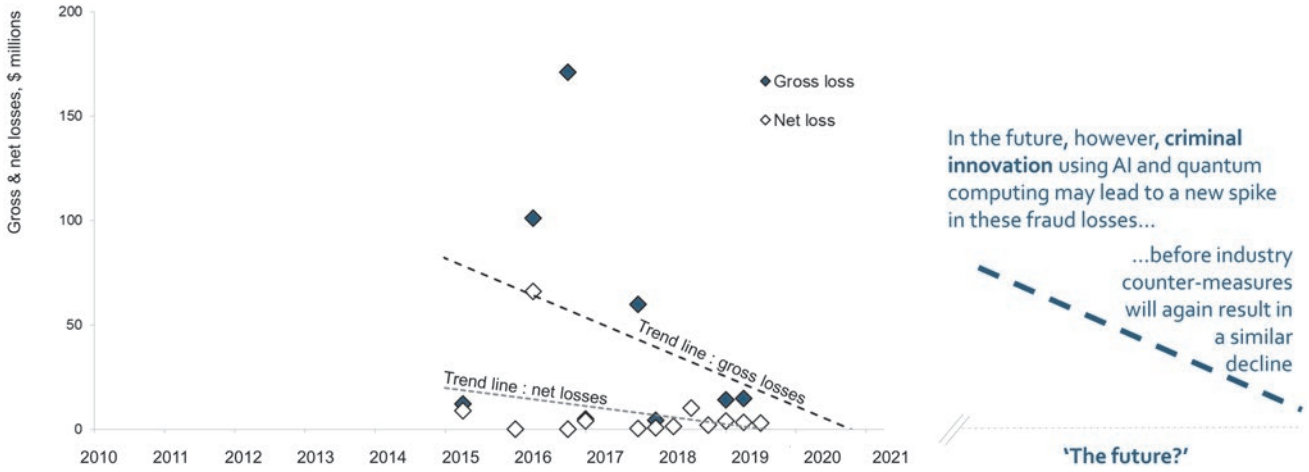

Figure 4: Gross and net losses from public SWIFT cyber-payment thefts over the last decade, and then looking into the future[43]

comforting level of control) the data of G-SIBs will increasingly be vulnerable through their third and fourth party relationships. For example, the customer data of multiple G-SIBs may have been compromised through the data theft from Equifax, the consumer credit agency, in 2017.

Digitisation has enabled bank robberies to be committed remotely. The first publicly disclosed Society for Worldwide Interbank Financial Telecommunication (SWIFT) cyber-payment theft seems to have taken place in 2015. The Bangladesh Bank theft in 2016 led to the transfer of five payments totalling US$101m. SWIFT and its roughly 11,000 members responded to these thefts with control enhancements. As a result, cyber-criminals evolved their techniques; after early 2018, the average fraudulent transaction amounts reduced by between 10× and 100× to between US$0.25m and US$2m.[42] In the future, however, criminal innovation using AI or quantum computing may lead to a new spike in these thefts, before industry counter-measures may again lead to a decline (Figure 4).

Adoption of cryptocurrencies as payment mechanisms seem quite limited. Thefts of cryptocurrency primarily from exchanges (eg the theft of ~US$200m from BitMart in 2021), a few trading platforms and, more recently, decentralised finance companies, however, do not seem to be declining in the same way that SWIFT cyber-payment thefts have declined based on details of thefts in the public domain.

In summary, AI and digitisation are creating new opportunities for cyber-criminals through the creation of concentrations of data and single points of failure, new ways of locating and exploiting victims more efficiently and the ability to circumvent bank controls, both now and in the future.

Conclusions

In advanced economies, incumbents have largely fought off the twin threats of BigTech and FinTech through digitisation, but this can increase the risks of disruption both during digital transformation and from the subsequent increased dependencies on third and fourth parties.

The new digitised end-state, through the automation of human processes, may lead to the replacement of random human errors (higher frequency but lower value losses) with systemic automated errors (lower frequency but higher value losses) arising from both catastrophic and silent failures. AI may also have the potential to be harnessed by either firms and/or their staff members to automate misconduct.

BigTech, by providing both software and IaaS, is creating new interconnectivity and dependencies which may lead to systemic disruption. BigTech may also lead to significant data leakage and breaches through its movement of data across borders.

AI may allow the enhancement of preventive and detective controls, for example, for monitoring of

financial crime, market misconduct and rogue trading by better and more efficiently identifying unusual patterns of behaviour. Cyber-criminals may, however, also harness these new technologies to circumvent banks' controls by using AI to produce deep-fakes such as voice-spoofing and quantum computing to break existing encryption. Cyber-criminals may also exploit customer and bank behaviour changes to optimise the proceeds from their crimes.

In aggregate, the digital revolution represents a very significant challenge to the operational risk management profession. Consequently, the next section considers the actions that they should be taking.

WHAT ACTIONS SHOULD OPERATIONAL RISK MANAGERS BE TAKING TO MITIGATE THESE RISKS

In the short-term, the digital revolution may drive a transient spike in operational risk events associated with the execution of digital transformation programmes as technology is advancing more rapidly than the control frameworks of banks through the usage of AI by staff members (eg the use of ChatGPT by several of Samsung's software engineers) and cyber-criminals (eg the use of voice-spoofing). Thereafter, the operational risk profiles of banks will continue to be dynamic as a result of the ongoing emergence of new technologies (eg quantum computing), the potential for AI model drift and changing stakeholder behaviours (Figure 1). There are no silver bullets for mitigating these risks (as seen in Table 1) and consequently, this section provides an overview of the portfolio of existing operational risk management control frameworks that need to be enhanced in the short and medium-terms to meet these threats.

Digital transformation

The not unreasonable expectation of the EU's Digital Operational Resilience Act (DORA) (2022) is that firms will appropriately manage 'each major change in the network and information system infrastructure'.[44] In practice this may involve:

- *stresses on BAU*: monitoring of a dashboard of metrics, highlighting trends in KRIs and KCIs focused on signs of stretch in a bank's BAU activities, eg lags in the performance of regular tasks, and growing back-logs in completing remedial actions to enhance controls;
- *risks of migration*: standard first line mitigations of migration/transition risks include governance, documenting business and functional requirements, project plans, RAID logs (risks, actions, issues and dependencies), non-functional and functional testing, migration run books, dress rehearsals and contingency planning. All of these activities reduce rather than eliminate the likelihood of failure;
- *weaknesses in interim and end-states*: risk assessments need to be undertaken on the interim and end-states to identify any new vulnerabilities that have been introduced and the effectiveness of work-arounds for any non-delivered functionality. When implementing vendor technology, firms must additionally focus not just on the functionality that they specified but also native functionality which may expose them to incremental operational risks.

As the second line cannot review all change initiatives, it needs to prioritise projects with hard migration dates, tight timescales and significant complexity and scale. Any 'Red' rated projects, should receive additional attention due to the temptation for project managers and sponsors to descope functionality, reduce the scope of testing, run formally sequential project tasks in parallel and re-rate the significance of bugs etc. Ultimately, the second line should critically review and challenge the first line's assumptions, assessments and activities regarding major change initiatives, calling out the inconvenient truths that are likely hiding in plain sight.

AI, including control enhancements

While AI has the potential to enhance the control frameworks and the efficiency of banks, they can clearly amplify existing risks and expose firms to new risks. Consequently, the use of AI, both informally by staff members and as part of digital

transformation, clearly needs to be formally governed. This involves firms articulating acceptable and unacceptable usage, defining the risk assessments that need to be undertaken and the approval processes, which should reflect the Prudential Regulation Authority's (PRA) recent Supervisory Statement on Model Risk Management.[45] Model validation is clearly a key component of any approval process of both internally developed and third party models and should variously include:

- *data quality validation* aimed at identifying incomplete, unrepresentative, biased and erroneous training data, eg to identify any biased/discriminatory lending;
- *outcome monitoring* against a benchmark or a non-AI model to ensure that the AI tool is equitable and free from bias;
- *'black box' testing*, which involves a developer experimenting with the model by feeding it different data inputs to better understand how the model makes its responses;
- *red-teaming*: The red-teamers *attack* the model, in an attempt to get it to do something inappropriate, as occurred with chatbot Tay.

While rigorous monitoring needs to be undertaken of any decision making tools, additional safeguards are required for AI due to the potential for model drift. These safeguards may include the following:

- *Alerts*: detective controls to flag unusual or unexpected actions to employees, to mitigate silent failures.
- *Human in the loop*: decisions are only executed after review and approval by a human.
- *Guardrails*: automatic termination of the AI if it produces undesired outputs. This is intended to mitigate model drift, which can occur with AI algorithms that are self-teaching.
- *Kill-switch*: to terminate rapidly if an AI algorithm is catastrophically malfunctioning.

While some of these controls are extensions of existing model/rules-based algo controls, others are new.

Third and fourth party suppliers

Both the EU's DORA and the UK's Discussion Paper on critical third parties[46] envisage a role for regulatory oversight of critical technology providers. In practice, even when firms have rights to access, inspect or audit a critical third party, banks cannot monitor their controls on a real-time basis. As a consequence, there needs to be increasing focus on business continuity management, disaster recovery and operational resilience, ie on contingency planning as to how firms will maintain important/critical business services for their customers if these critical suppliers suffer disruption as well as the processes for severing and restoring connectivity, for example, once the third party has recovered from a cyber-attack. DORA envisages that these plans are tested at least annually to ensure their effectiveness. Firms should also periodically review the data that they hold with third parties to ensure that it is minimised (ie that superfluous data is not being held with third or fourth parties) in terms of both volume and age. While firms should also have exit strategies for their third and fourth parties, these must identify the timescales for exit, for example, the duration of a migration from one datacentre operator to another would be measured in months, if not years, meaning that firms must have adequate redundancy/contingency because exit is not a viable short-term contingency arrangement. The move towards more regulatory oversight of critical technology providers is reflective in that the existing concentration in service provision, ie disruption, could potentially be the source of a future banking crisis.

Criminal innovation and control degradation

Ongoing criminal innovation (see Figures 3 and 4) will require banks to be perpetually vigilant and to be sharing data to identify new forms of attack, eg voice-spoofing. This requires banks to be dynamically assessing themselves against industry cyber-security standards, such as NIST, and identifying and mitigating new attack vectors and future threats through implementing quantum-safe encryption. DORA encourages banks to enhance their digital operational resilience through sharing

information on cyber threats, therefore slowing the ability of a new threat to spread, supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages.

Anecdotally, the speed of these changes feels like it is accelerating. This requires banks to be both very vigilant of the changes happening around them and extremely agile in their decision making. All of these activities will require additional digitally-skilled resources to be operating in first, second and third lines of defence, although in the short-term demand for these digital resources will outstrip supply.

CONCLUSION

The digital revolution is unstoppable and will transform banking (Figure 1) and as a consequence the operational risk profiles of banks (Table 1). There is no silver bullet to mitigate these risks; instead, a portfolio of existing control frameworks needs to be enhanced — ie change management, model risk management, third party vendor management, business continuity management, disaster recovery and operational resilience and cyber security — to address both the amplification of existing risks and also new risks associated with AI. The digital revolution may be a key driver of the operational risk losses of banks in the next decade, and the concentration of critical technology providers could potentially be the source of a future banking crisis.

AUTHOR'S NOTE

The contents of this paper are the author's own views rather than those of ICBC Standard Bank.

References and notes

1 OECD (2020) 'Digital Disruption in Banking and its Impact Competition', available at http://www.oecd.org/competition/digital-disruption-in-banking-and-its-impact-on-competition-2020.pdf (accessed 5th November, 2023).
2 UK Parliament House of Commons Library (1st September, 2023) 'Statistics on Access to Cash, Bank Branches and ATMs', available at https://commonslibrary.parliament.uk/research-briefings/cbp-8570/ (accessed 5th November, 2023).
3 *Ibid*.
4 M-Pesa is used by ~90 per cent of Kenyan households. *The Economist* (20th May, 2023) 'Cashless talk', available at https://www.economist.com/special-report/2023-05-20?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18156330227&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gad_source=5&gclid=EAIaIQobChMIldqYnOPPggMVkpFQBh1WfwNXEAAYAiAAEgKXOvD_BwE&gclsrc=aw.ds (accessed 24th November, 2023).
5 Bank of International Settlements (2019) 'Big Tech in Finance: Opportunities and Risks', available at https://www.bis.org/publ/arpdf/ar2019e3.htm (accessed 5th November, 2023).
6 Financial Stability Board (9th December, 2019) 'BigTech in Finance: Market Developments and Potential Financial Stability Implications', available at https://www.fsb.org/2019/12/bigtech-in-finance-market-developments-and-potential-financial-stability-implications/ (accessed 5th November, 2023).
7 Deloitte's Center for Financial Services March 2022 digital banking survey of 3,000 US consumers, weighted inline with the banking population found that millennials and Gen Z were respectively only 62 per cent and 57 per cent *satisfied* or *very satisfied* with their banks, and 28 per cent and 20 per cent respectively were *somewhat* or *very likely* to switch whilst for baby boomers and older generations the comparable data was 81 per cent and 85 per cent and 6 per cent and 1 per cent respectively. Valenti, J. and Alderman, R. (7th September, 2021) 'Building on the Digital Banking Momentum', Deloitte Insights, Issue 30, Summer 2022, available at https://www2.deloitte.com/xe/en/insights/industry/financial-services/digitalization-in-banking.html (accessed 5th November, 2023).
8 McKinsey & Co found that 40 per cent of US financial decision makers have a FinTech Account, and that younger FinTech users tend to use multiple accounts, whereas older generations are more likely to use just one FinTech account. Gen Z are the most frequent users of FinTech with 29 per cent having more than one account.

This is ~50 per cent of all Gen Z FinTech users. Krivkovich, A., White, O., Townsend, Z. and Euart, J. (17th December, 2020) 'How US Customers' Attitudes to Fintech are Shifting During the Pandemic', McKinsey & Co, available at https://www.mckinsey.com/industries/financial-services/our-insights/how-us-customers-attitudes-to-fintech-are-shifting-during-the-pandemic (accessed 5th November, 2023).

9 Netzer, A. (3rd February, 2021) 'How Millennials and Gen Z Could Reinvent the Banking Industry', Forbes, available at https://www.forbes.com/sites/forbescommunicationscouncil/2021/02/03/how-millennials-and-gen-z-could-reinvent-the-banking-industry/?sh=45fa6ec14e14 (accessed 5th November, 2023).

10 JPMorgan Chase & Co (2016) '2016 Annual Report', p. 49, available at https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/2016-annualreport.pdf (accessed 5th November, 2023).

11 OECD, ref 1 above.

12 Grimwade, M. (2019) 'Applying Existing Scenario Techniques to the Quantification of Emerging Operational Risks', *Journal of Operational Risk*, Vol. 14, No. 3, pp. 27–72.

13 This figure is adapted from Grimwade, M. (31st December, 2021) 'Ten Laws of Operational Risk: Understanding Its Behaviours to Improve Its Management', Wiley & Sons, Chichester, available at https://onlinelibrary.wiley.com/doi/book/10.1002/9781119841388 (accessed 5th November, 2023).

14 Bank of England and FCA (16th October, 2019) 'Machine Learning in UK Financial Services', available at https://www.bankofengland.co.uk/report/2019/machine-learning-in-uk-financial-services (accessed 5th November, 2023).

15 Bank of England (11th October, 2022) 'DP5/22 – Artificial Intelligence and Machine Learning', available at https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence (accessed 5th November, 2023).

16 *Ibid*.

17 Dastin, J. (10th October, 2018) 'Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women', Reuters, available at https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G (accessed 5th November, 2023).

18 NIST (19th December, 2019) 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software', available at https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software (accessed 5th November, 2023).

19 Kaye, B. (5th April, 2023) 'Australian Mayor Readies World's First Defamation Lawsuit over ChatGPT Content', Reuters, available at https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05/#:~:text=SYDNEY%2C%20April%205%20(Reuters),against%20the%20automated%20text%20service (accessed 5th November, 2023).

20 Blythe, L. and Sims, Z. (5th July, 2019) 'The Case of the Robot and the $23 Million – Who to Sue When Things Go Wrong?', Russell McVeagh, available at https://www.russellmcveagh.com/insights/july-2019/the-case-of-the-robot-and-the-23-million-who-to-su (accessed 5th November, 2023).

21 Last look enables firms to ensure that high frequency traders have not detected a move in a market a few milliseconds before the bank, enabling them to arbitrage the bank's marginally less nimble trading platforms. This is achieved by imposing a hold period between the receipt of a customer's order and its acceptance and execution.

22 NYDFS announces Barclay to pay additional $150m penalty, terminate employee for automated, electronic FX trading misconduct. New York DFS (18th November, 2015) 'Consent Order Under New York Banking Law §44', available at https://www.dfs.ny.gov/system/files/documents/2020/04/ea151117_barclays.pdf (accessed 5th November, 2023).

23 FSA (28th June, 2005) 'Final Notice: Citigroup Global Markets Limited', available at https://www.fca.org.uk/publication/final-notices/cgml_28jun05.pdf (accessed 5th November, 2023).

24 *The Economist* (23rd June, 2016) 'Frankenstein's Paperclips', available at https://www.economist.com/special-report/2016/06/23/frankensteins-paperclips (accessed 5th November, 2023).
25 *The Guardian*, (26th March, 2016) 'Microsoft "Deeply Sorry" for Racist and Sexist Tweets by AI Chatbot', available at https://www.theguardian.com/technology/2016/mar/26/microsoft-deeply-sorry-for-offensive-tweets-by-ai-chatbot (accessed 5th November, 2023).
26 Financial Conduct Authority (22nd November, 2017) 'FCA Fines Bond Trader £60,000 for Market Abuse', available at https://www.fca.org.uk/news/press-releases/fca-fines-bond-trader-60k-market-abuse#:~:text=Mr%20Walter's%20behaviour%20constituted%20market,financial%20penalty%20on%20Mr%20Walters (accessed 5th November, 2023).
27 Dreibelbis, E. (7th April, 2023) 'Samsung Software Engineers Busted for Pasting Proprietary Code Into ChatGPT', PCMAG.com, available at https://uk.pcmag.com/news/146345/samsung-software-engineers-busted-for-pasting-proprietary-code-into-chatgpt (accessed 5th November, 2023).
28 Byung-yuel, B. (3rd April, 2023) 'Korean Companies Scramble to Issue Guidelines for ChatGPT Over Data Leak Fears', *Korea Times*, available at https://www.koreatimes.co.kr/www/tech/2023/11/129_348342.htmlhe (accessed 5th November, 2023).
29 Cumbley, R. and Church, P. (6th April, 2023) 'ChatGPT – Is it Legal?', Linklaters, available at https://www.linklaters.com/en/insights/blogs/digilinks/2023/april/chatgpt---is-it-legal (accessed 5th November, 2023).
30 Adams, N.-R. (9th December, 2022) 'ChatGPT: Legal Issues with the World's Latest Augmented AI', Michalsons, available at https://www.michalsons.com/blog/chatgpt-legal-issues-with-the-worlds-latest-augmented-ai/62520#:~:text=Bias%20and%20discrimination&text=This%20means%20that%20ChatGPT%20could,to%20prevent%20bias%20and%20discrimination (accssed 5th November, 2023).
31 Brittain, B. (6th February, 2023) 'Getty Images Lawsuit say Stability AI Misused Photos to Train AI', Reuters, available at https://www.reuters.com/legal/getty-images-lawsuit-says-stability-ai-misused-photos-train-ai-2023-02-06/ (accessed 5th November, 2023).
32 Financial Stability Board, ref 6 above.
33 A Bank of England survey in 2020 estimated that more than 70 per cent of the 30 banks surveyed and 80 per cent of the 27 insurers surveyed, relied on just two cloud providers. Bank of England (17th January, 2020) 'How Reliant are Banks and Insurers on Cloud Outsourcing?', available at https://www.bankofengland.co.uk/bank-overground/2020/how-reliant-are-banks-and-insurers-on-cloud-outsourcing (accessed 20th November, 2023).
34 European Data Protection Board (22nd May, 2023) '1.2 billion Euro Fine for Facebook as a Result of an EDPB Binding Decision', available at https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en#:~:text=Brussels%2C%2022%20May%20%2D%20Following%20the,Protection%20Authority%20(IE%20DPA) (accessed 20th November, 2023).
35 Stupp, C. (30th August, 2019) 'Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case', The Wall Street Journal, available at https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (accessed 5th November, 2023).
36 White House Memorandum (4th May, 2022) 'National Security Memorandum on Promoting United States Leadership in Quantum Computing while Mitigating Risks to Vulnerable Cryptographic Systems', available at https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf (accessed 5th November, 2023).
37 Harishankar, R., Schaefer, J., Osborne, M., Muppidi, S. and Rjaibi, W. (2nd December, 2022) 'Security in the Quantum Computing Era', IBM Institute for Business Value, available at https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe-encryption (accessed 5th November, 2023).

38 Jurgens, J., Kohn, I. and Soutar, C. (September, 2022) 'Transitioning to a Quantum-Secure Economy', Word Economic Forum, available at https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf (accessed 5th November, 2023).
39 Bernasco, W. (2009) 'Foraging Strategies of Homo Criminalis: Lessons from Behavioural Ecology', *Crime Patterns and Analysis*, Vol. 2, No. 1, pp. 5–16.
40 The Depression-era American bank robber Willie Sutton, when asked why he robbed banks replied 'because that's where the money is!'
41 Information is Beautiful (September, 2022) 'World's Biggest Data Breaches & Hacks', available at https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (accessed 5th November, 2023).
42 SWIFT (April, 2019) 'Three years on from Bangladesh, Tackling the Adversaries', available at https://www.swift.com/swift-resource/210491/download?language=en (accessed 20th November, 2023).
43 Adapted from Grimwade, ref 13 above.
44 Article 8 of the EU's Digital Operational Resilience Act (DORA), November, 2022, available at https://www.digital-operational-resilience-act.com/DORA_Articles.html (accessed 5th November, 2023).
45 Bank of England PRA (May, 2023) 'Model Risk Management Principles for Banks, Supervisory Statement SS1/23', available at https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2023/ss123.pdf (accessed 5th November, 2023).
46 Bank of England (21st July, 2022) 'DP3/22 – Operational Resilience: Critical Third Parties to the UK Financial Sector. PRA Discussion Paper 3/22; FCA Discussion Paper 22/3', available at https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector (accessed 5th November, 2023).