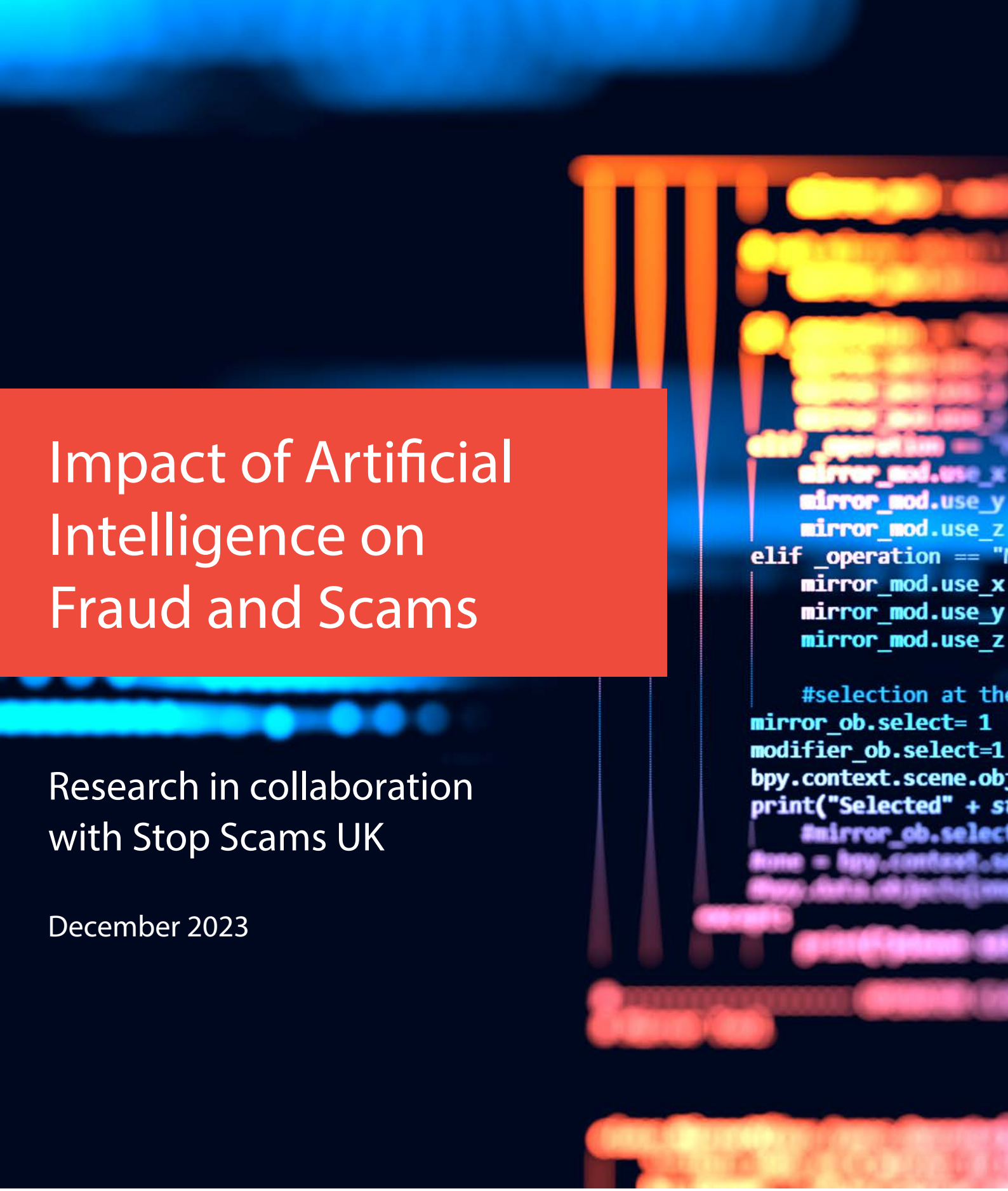


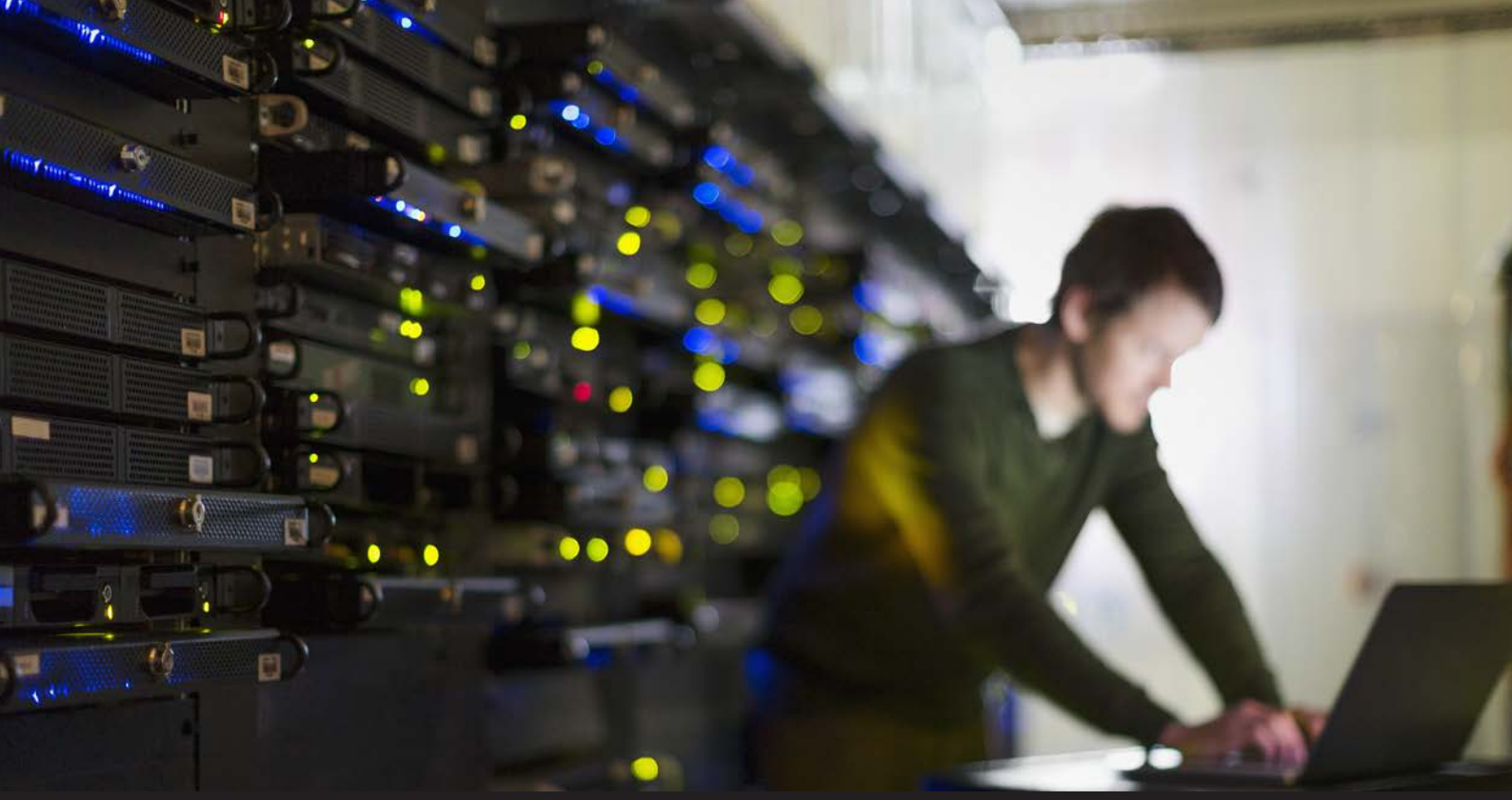
Impact of Artificial Intelligence on Fraud and Scams

Research in collaboration with Stop Scams UK

December 2023

pwc

STOP SCAMS UK



Contents

Foreword by Stop Scams UK

AI has captured the public imagination like few technologies before. Media has delighted in stories about what it may be able to do and its ability to generate new content almost instantaneously. Government leaders have met to debate whether AI poses an existential threat to us all, or at the very least forms of work as we know them. They have asked what should be done about it, whether it should be regulated and in what way.

In October 2023, Stop Scams UK organised a summit meeting hosted at the Bank of England by the Governor, Andrew Bailey, which brought together senior policy makers and representatives of industry. Our ambition was to move beyond the headlines and hyperbole and look at the real-world implications of fraud on AI. This report, and the research that underpins it undertaken by PwC together with Stop Scams UK's members, formed the basis for that discussion, bringing focus and real-world experience to understandings of the impact of AI on fraud.

We wanted to understand not just the threats AI might pose, but the real opportunities that it will bring for helping get a grip on the scam emergency. As the contributions to this report makes clear, AI will make it easier for criminals to perpetrate sophisticated scams at scale, and to impersonate trusted institutions, friends and family members, raising serious questions around trust in content. But as is made equally clear, AI will better enable banks and others to identify and prevent fraud and scams. Chatbots will engage with chatbots uncovering critical information about criminal operations. And AI will free up the time of specialist investigators to focus on those most difficult cases.

As a membership organisation of responsible businesses drawn from across the banking, technology and telecoms sectors that have come together to stop fraud and scams at source, Stop Scams UK was well placed to convene this debate. Our members are not just at the forefront of the fight against fraud and scams, they are also at the cutting edge of the development of AI. They are the very people and organisations who need to contribute to the formation of policy to ensure that we get the framework right so that AI is harnessed as a force for good.

As we go forward, Stop Scams UK and its members have committed to work together to monitor emerging threats and opportunities and share best practice, insight and intelligence, which will help firms stay ahead of the fraudsters and keep their customers and consumers safe.

We are very pleased to have worked with PwC on this research and to continue this work over the coming months. PwC has brought a global perspective to this complicated issue. This report is the result of partnership and collaborations, across sectors and technologies. It is our belief that it is only by working in partnership that we will see a significant reduction of fraud and scams in the long term.

- Ruth Evans, Chair Stop Scams UK

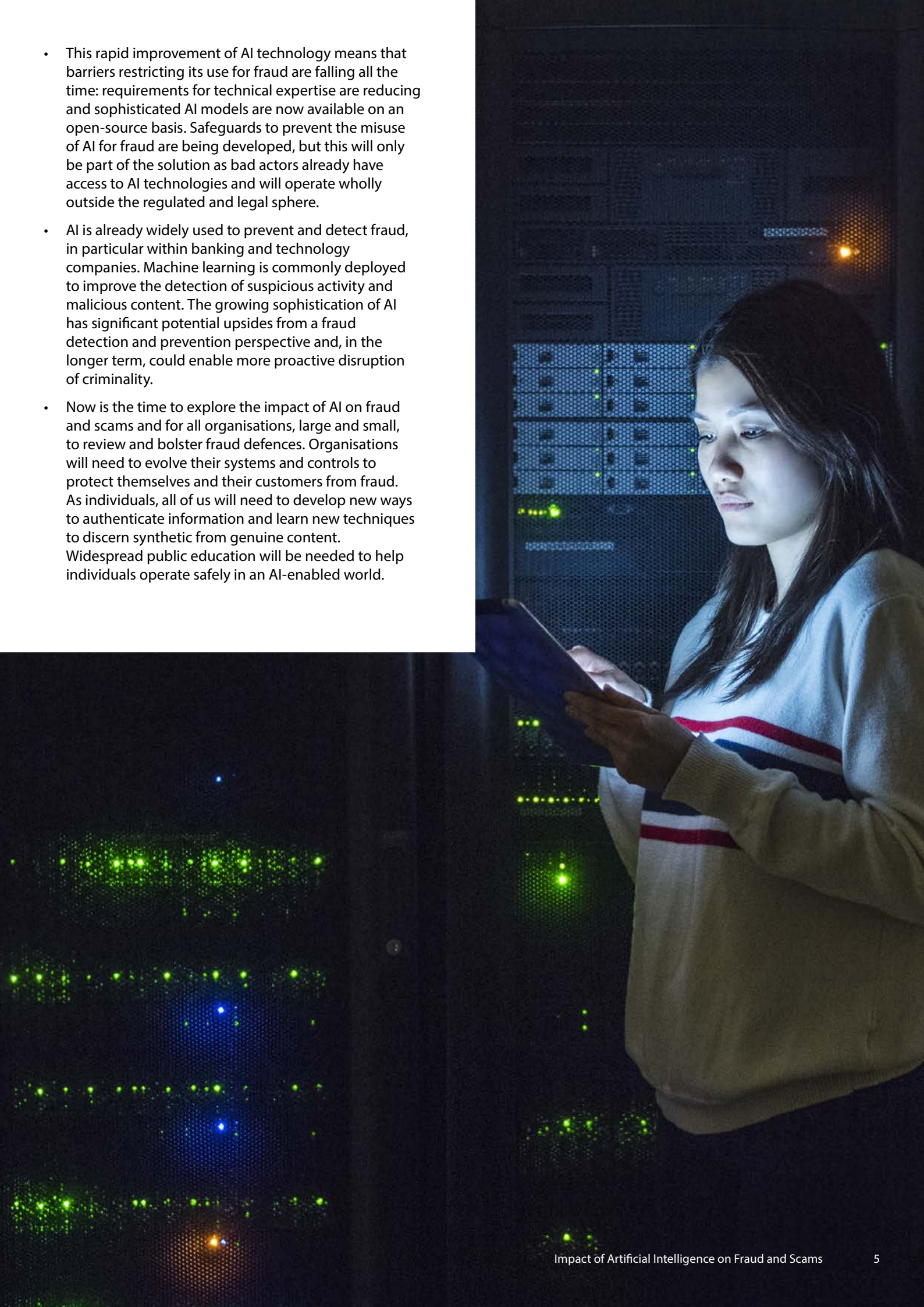
STOP SCAMS UK

Headline findings

> AI will have wide reaching impacts across the whole of society and has the potential both to create significant harm but also to drive significant improvement across a wide range of applications. PwC's research highlights that while there is limited evidence that AI is behind large numbers of fraud attacks now, it will very likely drive an increase in the number and sophistication of fraud threats. The time to act to safeguard our society from AI-enabled fraud is now, and all organisations need to think carefully about how AI may create fraud risks for their business and their customers. This will require ongoing vigilance, including monitoring and the sharing of insight and best practice between firms and across sectors."
>
> - Andrew Bailey, Governor of the Bank of England.

- AI has extraordinary potential to drive positive change across all areas of business and society. Use cases span medical research, tackling climate change and improving access to nutrition as well as driving improved efficiency and effectiveness of business processes across all industry sectors. However, as is often the case with new technologies, there will be negative impacts of AI and ways that it will be misused.
- The use of AI to perpetrate fraud and scams is one such likely misuse. PwC has collaborated with Stop Scams UK to explore how AI technology impacts fraud and scams to gather insight to support strategic planning across the public and private sectors to defend against AI-enabled fraud threats. Our research has involved speaking to those closest to the issues: senior leaders from major UK banks, representatives from global technology companies (including those developing leading-edge AI tools), and telecommunications operators as well stakeholders from regulators, cross-sector research organisations and representatives from government.
- Our research was presented at a first-of-its-kind cross-sector AI fraud summit event hosted at the Bank of England. This paper summarises the results of our research and the key themes discussed during the summit.
- There is consensus that AI will drive an increase in the volume and sophistication of fraud and scams. Businesses are already making use of AI techniques for fraud prevention and those we spoke to as part of our research have a keen eye on the changing fraud threats presented by emerging AI technology.
- While there have been widely reported cases of AI being used to perpetrate fraud and scams already, there is little evidence so far that this is happening at scale. The banks we spoke to had limited evidence that AI had been used to perpetrate fraud, although they called out that it can be difficult to identify the use of AI as compared to human-generated scams.
- Some technology companies we spoke to were clear that AI is being used to generate fake content and create malicious user profiles. There was agreement across all the participants in our research that it is only a matter of time before fraudsters adopt AI for fraud and scams at scale, but there were a range of views about the immediacy of this threat. Those closest to the development of AI technology tended to talk about threats in timescales of weeks and months, pointing to the rapid evolution of the technology and the challenges of staying up to date on its capabilities.

- This rapid improvement of AI technology means that barriers restricting its use for fraud are falling all the time: requirements for technical expertise are reducing and sophisticated AI models are now available on an open-source basis. Safeguards to prevent the misuse of AI for fraud are being developed, but this will only be part of the solution as bad actors already have access to AI technologies and will operate wholly outside the regulated and legal sphere.
- AI is already widely used to prevent and detect fraud, in particular within banking and technology companies. Machine learning is commonly deployed to improve the detection of suspicious activity and malicious content. The growing sophistication of AI has significant potential upsides from a fraud detection and prevention perspective and, in the longer term, could enable more proactive disruption of criminality.
- Now is the time to explore the impact of AI on fraud and scams and for all organisations, large and small, to review and bolster fraud defences. Organisations will need to evolve their systems and controls to protect themselves and their customers from fraud. As individuals, all of us will need to develop new ways to authenticate information and learn new techniques to discern synthetic from genuine content. Widespread public education will be needed to help individuals operate safely in an AI-enabled world.



Introduction

While headline rates of fraud remain very high, progress is being made to tackle fraud and scams in the UK. The rapid increase in fraud losses, driven by the rise of scams over the last five years in particular, and action by groups like Stop Scams UK (and their members) have galvanised a stronger collective fraud response: the government has published a National Fraud Strategy; banks and payment firms are investing in better fraud defences; and new obligations introduced through the Online Safety Act and commitments in sector fraud charters are bringing technology companies and telecommunications operators more directly into the counter-fraud world. Recent statistics show encouraging, although early, signs that collective measures are having an impact.

A key consideration is how to sustain this positive direction of travel, building greater resilience into our collective counter-fraud response and evolving fraud countermeasures at the pace needed to keep up with technological change. AI presents the most significant challenge in this regard. The speed with which AI capabilities are improving is astonishing and there is a real risk that hard-fought improvements in fraud defences could be undone if the right measures are not put in place to defend against fraud in an AI-enabled world.

PwC has collaborated with Stop Scams UK to explore how AI technology impacts fraud and scams and to gather insight to support strategic planning across the public and private sectors to defend against AI-enabled fraud threats.

During September and October 2023, we spoke with a number of Stop Scams UK members including representatives from seven leading UK banks, three of the largest global technology companies and one major telecoms operator. Our role was to collate views across participants and identify key cross-sector themes. To inform our summary, we also leveraged PwC's own fraud and financial crime specialists, as well as our dedicated team of AI experts to understand how AI is driving fraud threats and its likely evolution in the short to medium term.

Our aim was to get a broad set of cross-sector perspective on three key questions:

1. How is AI currently being used by fraudsters?
2. How is AI currently being used to prevent and detect fraud and scams?
3. What opportunities might there be to use AI to strengthen fraud response in the future?

In answering these questions, our research has sought to cut through the hype and provide an evidenced-based assessment of the current risks and challenges as well as reflecting on the significant potential upsides that AI could deliver, if harnessed correctly, to prevent, detect and disrupt fraud.

The headline messages from our research were presented at a Stop Scams summit event on 6 October 2023 hosted at the Bank of England and chaired by the Governor, Andrew Bailey. The summit was attended by industry leaders from some of the largest UK banks, representatives from key regulators, and representatives from the biggest global technology and telecommunications companies. Senior government officials from the Home Office and Treasury also attended as well as the Prime Minister's fraud champion, Anthony Browne MP.

This first-of-its-kind cross-sector summit event on the impact of AI on fraud and scams demonstrated the willingness and desire across industry sectors to tackle issues of fraud generally, but also to take the right action now to develop safeguards against the misuse of AI for fraud. The discussion amongst the group recognised the potential threats from AI, while also considering the significant potential of AI to tackle fraud and scams and the transformational impact of the technology. A key challenge discussed during the event was how to implement the right protective measures without stifling innovation. Three key themes emerged from the discussion that we explore in this paper:

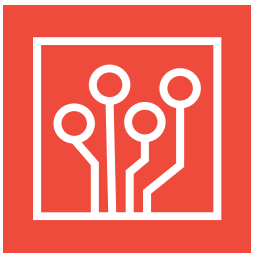
1. Industry vigilance - continuing to monitor AI's impact on fraud and scams.
2. Adaption and agility - preparing to adapt swiftly to evolving threats, both at an individual organisation level, but also nationally and across the global community.
3. Cross-sector collaboration - Working together across technology, telecommunications, the banking sectors and with the government to develop safeguards and to maximise the benefits of AI development.

Development of AI

AI is an umbrella term, representing a range of algorithm-based technologies that solve complex tasks by carrying out analytical functions that previously required human brain power. AI technologies have been available for a number of years, however, recent innovations, such as ChatGPT and MidJourney, have pushed the technology into the public eye and have, for the first time, enabled easy access to powerful tools through an intuitive interface that anyone can use.

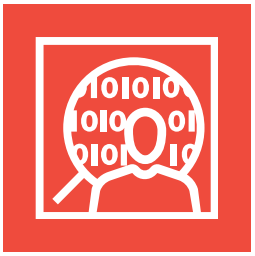
The world of AI is vast and represents a range of technical innovations. Below we highlight some key AI concepts, techniques and examples of their usage:

Machine learning - Machine learning represents a broad array of algorithms where a computer uses statistical models to analyse and draw inferences from patterns in data. Over time, the model gets better at a given task by learning to recognise patterns by being shown a large number of different examples of a given subject. For example, online shopping sites are better able to recommend products to a customer based on a longer history of browsing and purchasing information.



Deep learning - Considered a subcategory of machine learning, deep learning uses 'virtual neurons' to simulate a brain-like structure to process vast amounts of information and store patterns. Examples of deep learning include virtual assistants such as Amazon's Alexa or Apple's Siri, where the algorithm is used to recognise voice commands.

Generative AI (GenAI) - Within deep learning there is a subcategory of algorithms called generative AI (also known as GenAI). GenAI takes advantage of the information stored in deep learning algorithms to combine patterns and create a desired output based on user prompts. The popular MidJourney app is an example of a text-to-picture GenAI that allows users to generate images based on written prompts, creating bespoke art forms.



Large Language Models (LLM) - Popularised as the technology that powers ChatGPT, LLMs are a type of GenAI that are fed enormous volumes of text to establish context and how words relate to one another in a given document. A user can then query this context and relationship model to generate a text-based output. For example, ChatGPT mimics human-like conversations, where its language model continuously builds a bank of data that allows the system to respond to questions.

Given the powerful abilities of these new AI tools, coupled with the ease and accessibility, AI has the potential to significantly disrupt existing industries and create unprecedented change. It is therefore easy to see how this technology could find applications in the world of fraud and scams, whether being used by a fraudster to develop more effective patterns of attack, or more positively, to support the more effective prevention and detection of fraud.

How is AI being used by fraudsters and how might threats change as AI evolves?

Across all the people we spoke to, there was agreement that AI will drive an increase in the volume and sophistication of fraud and scams.

The organisations our participants represent already have a keen eye on the fraud threats presented by AI with some taking steps to bring AI specialists into fraud-focused teams and others having business-wide programmes to gather perspectives on AI opportunities and threats, including those related to fraud.

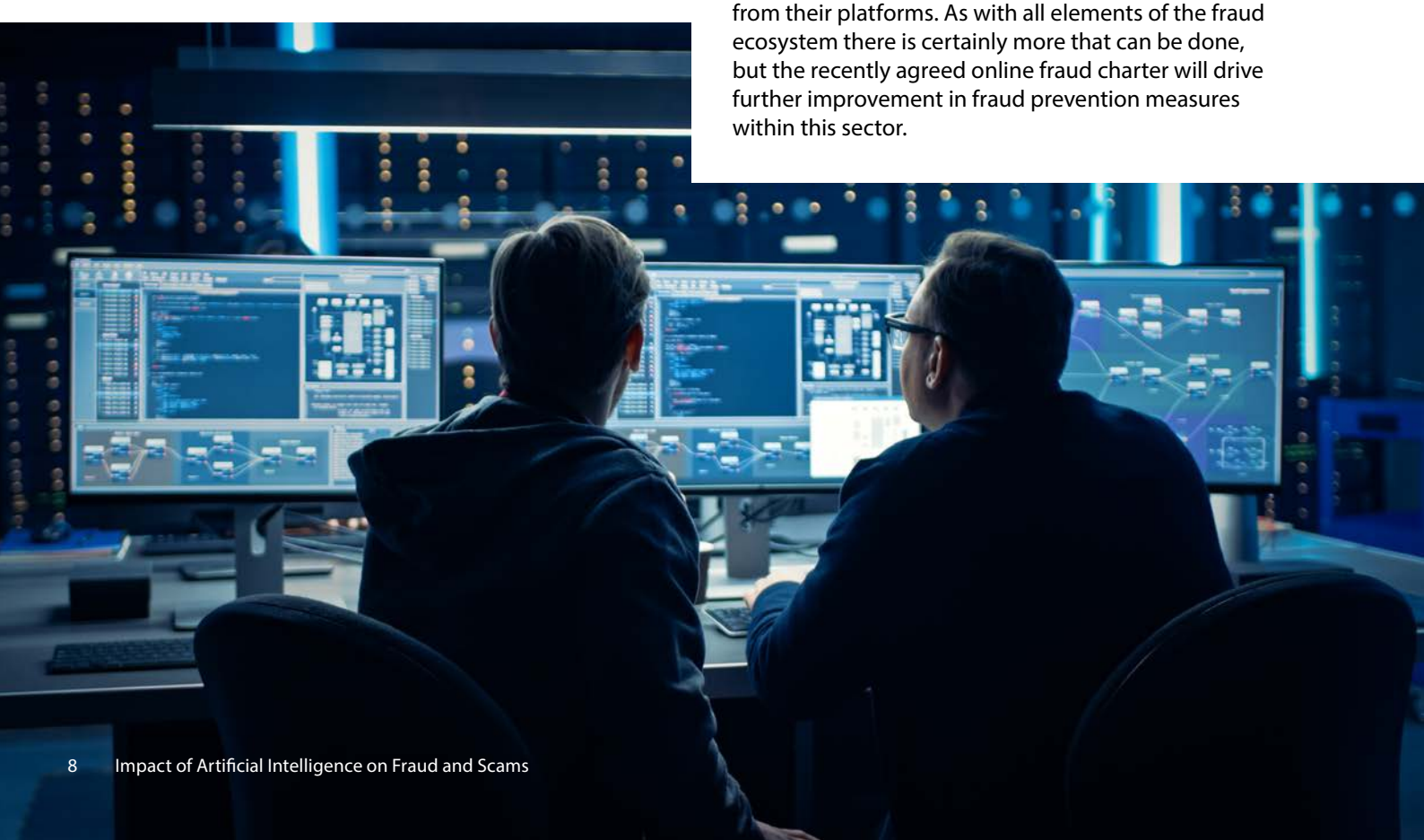
It was acknowledged that there have already been widely reported cases of AI being used to perpetrate fraud and scams. Publicly reported examples include cases where voice clones appeared to have been used to perpetrate a scam against a UK-based energy company and a fake kidnapping in the US, as well as several cases where deep fake videos of celebrities had been used to promote investment scams, including a case involving a deep fake of Martin Lewis, the money savings guru. Banks we spoke to also described a small number of cases that had not been publicly reported where they believe AI may have been behind attempted and actual fraud cases within their own businesses.

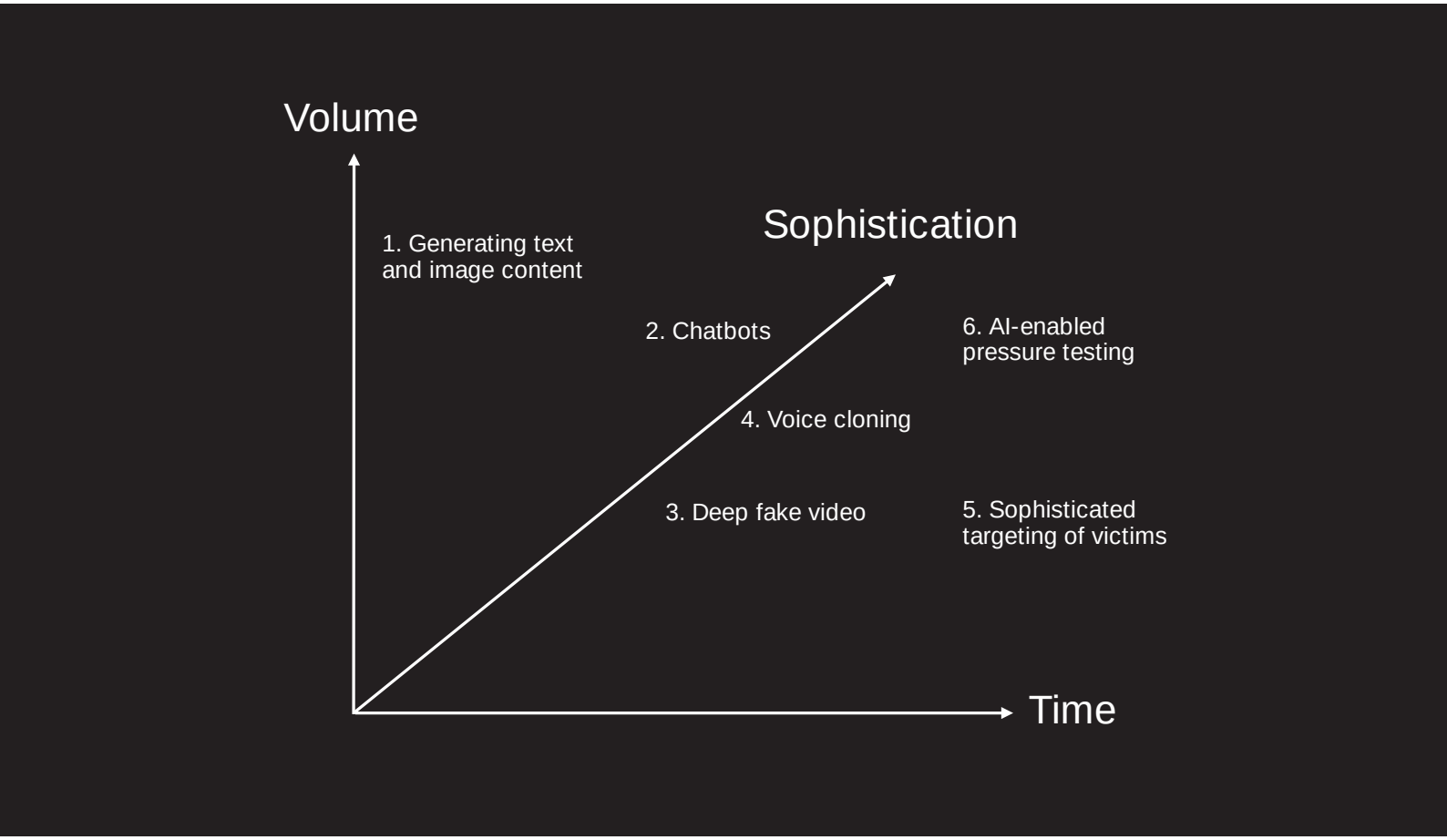
So while it is clear that AI is already being used by fraudsters, none of the banks we spoke to had evidence that this was currently happening at scale with very small numbers of cases identified to date relative to the more than three million cases of fraud in 2022 in the UK alone.

A key challenge to assessing the current threat posed by AI is the difficulty in determining whether a scam has involved AI or not. AI content (whether text or images) is not easily discernible from human-generated content without specialist tools. Identifying that AI was behind a fraud or scam is largely down to context and potential flaws in the scam approach that might be spotted by an experienced eye leading to more thorough investigation. It is possible that other scam cases have involved fraudsters using AI tools without this being identified. There is also no standardised reporting or data collection on AI-enabled fraud further limiting our ability to conclude definitively that AI is not currently being used extensively by fraudsters.

One reason why fraudsters may not yet be adopting AI techniques is that they continue to be highly successful perpetrating scams using traditional techniques. Our research highlights that it is highly likely that fraudsters will increasingly adopt AI tools to perpetrate fraud and scams, but this may only happen at scale when preventative measures force fraudsters to develop new approaches to maintain their success at capturing and manipulating victims.

Some technology companies that we spoke to were much more certain that AI is already being used to generate fake content and create malicious user profiles. Extensive work is already being done by these companies, often using elements of machine learning, to identify harmful content and remove this from their platforms. As with all elements of the fraud ecosystem there is certainly more that can be done, but the recently agreed online fraud charter will drive further improvement in fraud prevention measures within this sector.





Our research has highlighted six key ways that AI tools could be used to perpetrate fraud and scams. Each of these methods have the potential to drive increases in fraud across two key dimensions:

- Volume - amplifying fraudsters' potential reach by enabling the generation of scam content at greater speeds and at scale.
- Sophistication - increasing success rates by enabling the creation of more convincing and personalised scam content.

For each of the six methods, we have also considered a third dimension, time, recognising that AI capabilities are evolving quickly with fraud use cases potentially emerging very rapidly.

Generating text and image content

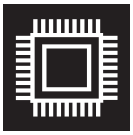
- GenAI can be used to create tailored emails, instant messages and image content as bait to hook potential scam victims, for example, in phishing and smishing attempts, or by creating fraudulent adverts.
- Some of the traditional 'tells' in these kinds of scams, like poor spelling and grammar, can be eliminated using AI making them much harder to detect.
- Thinking more broadly than scams, GenAI can also be used to create fabricated images, for example of damaged vehicles or property, in support of insurance claims.
- While some GenAI tools contain safeguards to prevent against this kind of misuse by design, participants of our research highlighted that these can be bypassed and that open source models could be used without these safeguards in place.
- Stakeholders we spoke to as part of our research believe that this is already likely to be a prevalent threat that will increase over time.

AI enabled chatbots

- Some of the organisations we spoke to already had evidence that sophisticated chatbots, that may be leveraging elements of AI, are being used to converse with potential scam victims as part of the process to manipulate them into making payments.
- Examples were cited where out-of-context questions had been intentionally put into chat conversations with scammers as part of intelligence gathering exercises which had led to unnatural responses that appeared to be computer generated.
- Chatbots have the potential to multiply fraudsters' ability to contact victims, without the need for extensive human involvement: a single chatbot could deliver the same scam volume that would previously have required a call centre of people.
- While there is limited evidence that this is happening at scale, our research participants expect this threat to increase. Chatbots will drive up fraud volume, with the detection of this threat becoming harder over time as AI becomes indistinguishable from humans.

Deep fakes video

- Deep fakes videos are already being used as a means of baiting potential victims. Examples were given where deep fake videos were being used as 'click bait' to drive traffic to malicious websites which harvest card payment details for subsequent use in payment fraud.
- As noted earlier, there are well reported cases where the image and persona of a trusted person has been used to encourage individuals to engage with malicious content.
- We also heard from one bank that uses 'selfie video ID' technology, that they have seen relatively unsophisticated examples of people using deep fake videos held up on screens in front of their web cameras to attempt to bypass 'selfie video ID' controls.
- The use of deep fake videos will become more prevalent and those we spoke to have a keen eye on how technology and behavioural changes will be needed to help individuals differentiate between trustworthy and untrustworthy content.



Voice cloning - scams and voice ID

- Deep fake technology has the power to clone voices to an increasingly high degree of accuracy. Currently, high quality voice clones can require up to a couple of hours of audio content to perfect but the requirement for training data is reducing over time.
- One technology company we spoke to believes that within months it will be possible to create a human indistinguishable voice clone from just seconds of audio content.
- There are already examples of voice cloning being used in scams where voice messages have been used, and in the short-term real time conversations with scammers using cloned voices is a very real possibility.
- The fraudulent applications can be easily imagined, for example: an employee receives a call from someone claiming to be the CEO and speaking in the CEO's voice, asking them to make a payment to another account.

- A shift in how we verify who we are speaking to, both with behavioural and technological changes, will be needed to protect ourselves from these kinds of frauds.
- We are also aware of at least one case where a voice clone was used successfully to penetrate a bank's voice biometric ID system. However, banks we spoke to felt that upgrades to their voice ID systems limited this risk and they noted that this was something they were extensively testing.
- Even so, views from technology companies were stronger that voice ID would need further enhancement to be a viable biometric authentication method in the future.

Sophisticated targeting of victims

- AI tools can be used to review large volumes of data to identify potential victims and tailor scam content to an individual's specific vulnerabilities, for example: identifying an individual's employment details or family circumstances or where they have recently been on holiday and tailoring messages to capture these details.
- While this kind of tailoring, so called 'spearfishing', is not new, being able to do this on an automated basis at scale is.
- There is no hard evidence that this is currently happening, but there was a belief amongst some of those that we spoke to that this risk will increase in prevalence over time.

Pressure testing

- Brute force attacks against bank systems - particularly on debit and credit cards in so-called BIN attacks - are nothing new and the industry has evolved mechanisms to prevent and detect these kinds of threats.
- As AI evolves, those we spoke to expect these kinds of attacks to grow in their sophistication with AI being used to flex attack patterns and to develop more subtle strategies to identify vulnerabilities that can be exploited.
- There is no evidence that AI is being used in this way yet but it is certainly a risk that organisations are taking seriously and considering how to develop more agile and sophisticated defensive strategies.

Across all of these threat types, research participants agreed that continued exploration of safeguards by design will be important but also that we need to continue hardening business processes through better preventative and detective measures (including capabilities powered by AI). Education and awareness will also be important to encourage the right behaviours to help individuals to identify untrustworthy content and communications and to operate safely in an AI-enabled world.

A common thread across these threat types is the use of AI to create content or trust with a potential victim, with the aim of deceiving them or manipulating them as part of a scam. In many respects, there is no difference in strategy for scam methods as compared to current human generated scam content. Similarly, the kind of fraudulent access to banking platforms that breach customer identification methods is a risk type that banks have managed for a long time and for which there are multiple layered protections. For technology platforms, the moderation of content, whether human or AI generated, is not a new challenge.

It is too soon to say what new fraud types will emerge, but currently similarities between AI and human generated scams mean that existing fraud defences can still be effective. While it might not be necessary to completely replace existing control methods, it will be important to continuously test and challenge whether fraud defences remain fit for purpose in an AI-enabled world. Fraud controls will need to be constantly evolved to combat new fraud types.

How is AI being used to prevent and detect fraud and scams?

> Machine learning techniques are generally already embedded in our fraud detection systems, reducing false positive rates and driving efficiency in our investigation teams while also improving our ability to spot suspicious activity. We are continuously evolving our detection models to improve detection capabilities with new data sets being used to spot more subtle indicators of fraud risk."
>
> - UK bank Head of Fraud

AI technologies have been around for a number of years and, in the case of many of the organisations we spoke to, are embedded in existing fraud defences.

The current primary use of AI in fraud defence is through the use of machine learning-based models to detect transactions, behaviours, activity or content that looks suspicious or outside of the norm.

Across the banking industry, it is common for historical data on fraud cases to be fed into machine learning models to enable behaviours or transactions with similar features to be more effectively identified as possible fraud. This kind of approach to monitoring is well embedded across card payments fraud detection and increasingly in models to detect potential payments to scammers to enable more effective, specific warnings to be given to customers at the point of payment. Technology companies and telecommunications operators also make extensive use of machine learning as part of network filtering (e.g. to block spam messages) and to identify and remove malicious content.

There is growing sophistication in the use of machine learning techniques with organisations exposing models to new data sets to enable more subtle indicators of fraud to be identified. Within banking specifically, machine learning is widely used to detect application fraud, digital fraud (e.g. remote banking fraud/account takeover) and payments fraud.

We also work closely with a number of technology vendors and alliance partners that provide AI tools to industry. These include AI-powered voice analytics tools that can identify risk in voices, complex network analytics platforms that use elements of machine learning to refine the identification of relationships between entities and AI-powered tools to identify manipulated image content. Across all areas of industry, organisations are exploring how AI can be used to improve fraud detection.

We have identified three key ways that AI can be better used to defend against fraud and scams

1

Improved detection

- There are a wide range of applications for AI in fraud and scam detection, for example: bank transaction monitoring; spam message filtering; harmful content blocking; and for the detection of malware.
- Continuous improvements are being made to enhance detection capabilities using machine learning and other AI approaches with increasingly sophisticated models being deployed to combine structured and unstructured data sets to provide more rounded views of high risk behaviours.
- One example of a more sophisticated detection approach being developed is the use of AI models to alert individuals where patterns of communication over time look like social engineering. For example, in the future, functionality like a spam filter could alert users or, in a business context corporate compliance teams, that an individual may be being targeted for social engineering.

2

Driving operational efficiency to free up investigative resources

- While much of the focus is on using AI to improve fraud detection systems, the benefit of using AI capabilities and automation more generally to free up expert capacity to focus on riskier areas should not be underestimated. For example, we see organisations using chatbots to close down simple customer queries, freeing up time for staff to manage more complex issues.
- Machine learning tools that filter false positives out of detection systems allow for better prioritisation of genuinely suspicious activity monitoring.
- In our view, in the shorter term, using AI for process efficiency gains is likely to have the biggest 'bang for buck' in terms of fraud prevention.

3

AI fighting AI

- AI tools are already being used to identify synthetic content such as fake images and voice clones. AI tools are also being developed to help distinguish trustworthy and untrustworthy content.
- We believe AI will increasingly be deployed to proactively protect users from malicious content and to take the fight to fraudsters.
- One example of how AI could be used to disrupt scams specifically would be developing chatbots to proactively engage in dialogue with fraudsters to waste their time but also to get them to provide information to enable tracing. Using chatbots to automate the collection of fraudsters' bank account information would provide a powerful intelligence source, if shared, for accounts to be investigated and fraudsters reported to law enforcement.

> In 2023, we partnered with Stop Scams UK to operate a proactive scam disruption pilot that led to more than 600 piece of intelligence being captured. Automating this capability, using AI-power chatbots could enable scam disruption at scale and provide valuable intelligence to identify fraudsters operating within our financial systems. AI also has the potential to streamline our operational processes and create more capacity for our fraud prevention teams to protect more customers from fraud"
>
> UK bank Head of Fraud.

Considerations for industry

AI will have wide reaching impacts across society that go beyond fraud and scams. There is ongoing exploration of how to build the right safeguards and protections into AI by design, involving both the public and private sectors. Earlier in 2023, the UK government hosted its AI Safety Summit to consider the risks posed by AI and how they can be mitigated through coordinated international action. The key output of the summit was a joint agreement from 28 participating countries on the risks and need for international action on frontier AI - the systems where the most urgent and dangerous risks are emerging. Sustained international co-operation on AI will be key as will public and private sector collaboration to address the risks posed by AI specifically in relation to fraud and scams.

If safeguards against the misuse of AI can be hardwired in the technology and steps are taken to educate the public on the impacts of AI more generally, perhaps the need for specific interventions to prevent misuse AI for fraud and scams may recede, notwithstanding that there will be a need for constant threat monitoring to enable rapid response.

Stop Scams UK is a cross-sector membership organisation that brings together banks, technology companies and telecommunications operators to develop new solutions to help stop fraud and scams at source. Building on discussions at the October summit at the Bank of England, Stop Scams UK is bringing forward a rapid response capability to share knowledge on the impact of AI on fraud and scams. This is a positive development. PwC will continue to play a part supporting this activity as well as our wider work supporting organisations to strengthen their fraud protections.

While international and cross-sector collaboration is important, there is also a lot that can be done to safeguard businesses and consumers from fraud risks within individual sectors and by individual organisations. The high levels of focus on fraud and scams at the moment is encouraging in this regard, and we are working across the banking, technology and telecommunications sectors to support organisations develop more effective counter-measures against fraud and scams. Better customer identification process, strengthened 'Know Your Client' practices and increasingly sophisticated threat detection are all important areas for improvement. We believe that there are three key areas to prioritise to address the risks of AI in relation to fraud specifically:

Education and awareness - Education and awareness will be a key challenge. As well as facing a barrage of fraudulent material and scam messages, there is also a lot of content on fraud awareness and personal protection. While these campaigns are positive, cutting through the noise, reaching consumers and, most importantly, changing behaviours is difficult. Coordination across the public and private sectors is needed to streamline messaging to provide clear, simple and consistent messaging around fraud generally, but also how AI may change fraud threats specifically. Ultimately, behavioural changes will be needed across our whole society with each of us adopting techniques to validate information presented to us. Education needs to start earlier, as part of schooling, to help individuals understand the warning signs of fraud.

AI is a powerful force for change and all of us - government, businesses, organisations and individuals - need to learn to change with it. While AI presents many threats and challenges, not least in relation to fraud and scams, it also presents a huge opportunity to improve our lives. As a tool to prevent and detect fraud, AI will be game changing. The challenge, as ever, will be to adapt quickly enough to keep pace with those seeking to use the technology maliciously.

Supporting trust through technology - Further technology developments will also be needed to support the wider trust agenda and we expect technology-enabled trust solutions to continue emerging to help individuals differentiate between trustworthy and untrustworthy content and communications. Technology can be used to provide prompts to warn consumers that a call, message or content might not be trustworthy and steps are already being taken to automate the identification of synthetic content generated by AI and alert users to this.

Evolution of counter-fraud controls - At a business level, fraud controls need to continuously evolve to counter emerging threats. This has always been the case, but the pace of development of AI will force businesses to accelerate processes to review and refresh counter-fraud controls. Businesses will need to develop frameworks and processes to test and challenge their controls, and legislation like the Economic Crime and Corporate Transparency Act, which introduces a failure to prevent fraud offence, will be helpful to encourage the right level of attention on fraud risk.

PwC contact details

Alex West

Banking and payments fraud leader

alex.e.west@pwc.com

+44 7841 567 371

Fabrice Ciais

AI risk specialist

fabrice.ciais@pwc.com

+ 44 784 333 4241