TACKLING AI SCAMMERS

The race is on to outfox deepfakes

As the limits of AI continue to expand beyond our immediate comprehension, what actions can banks take to mitigate the risk from cybercriminals intent on deceiving customers and disrupting the business world?

Artificial intelligence (AI) is changing the banking landscape, for better or for worse it still remains unclear. While there are opportunities on the horizon across multiple sectors, the more pressing issue for FIs is not only the risk to their own infrastructure and security but that of their customers.

"We are currently in the middle of an AI storm. It hasn't been around for that long, is developing quickly, and needs to be harnessed in a way that's safe to do so," explains Christian Garcia, CEO, Trusted Novus Bank.

The devil is in the data

Today AI can generate compelling content in multiple media formats. Better written text or authentic audio may be more believable to our eyes and ears, but data scrutiny may reveal otherwise. Dr Viktor Dörfler, Professor of AI Strategy, University of Strathclyde explains that generative AI (gen AI) 'hallucination' – whereby AI creates false information – is not a convincing concept, because it suggests that AI is making the wrong predictions based on incorrect or biased data. "This is wrong for two reasons. First, it is human to hallucinate, and we shouldn't attribute it to AI. Second, it suggests that something isn't working properly," he explains.

Human beings make relative assumptions based on their own interpretations of information that is not necessarily valid. Similarly, AI does exactly what it is programmed to do. "The essence of gen AI is to observe input patterns and then generate patterns that are similar to the ones served as input," says Dörfler.

AI output can only be as sophisticated as the data input by criminals – the humans behind the technology. "However, the more digital traces we leave online, the more data there is available for criminals to use to train these AI tools," says Jochem Hummel, Assistant Professor, Information Systems Management and Analytics Group, Warwick Business School.

Sorting out the fact from fiction

As the sophistication of AI increases, it may become more difficult for banks and customers to differentiate between a fake and the real thing. "Not only can AI impersonate a banker, but also friends and family. It can even emulate you as a person," cautions Hummel.

"Banks also may have to contend with the clever falsification of documents; AI has the ability to create fictitious documentation that supports the identity of an unreal person – in essence, a documented life," says Garcia.

Believing something that doesn't exist is the bedrock of the AI threat to UK banking. "Replicating someone's voice is incredibly easy with AI. Even a few minutes of a voice sample from someone means the fake will be so good that, even if you know that person in real life, you might not realise it isn't that person. But you may well recognise disparities in the wording," says Dörfler. The style of how someone talks is an entirely different issue, which is why the gen AI element is so important. "You may recognise that the person you know doesn't speak in that way or use those phrases in sentences," concludes Dörfler.

Augmentation, the collaboration between AI automation and human expertise, is where the real risk lies. "While automation creates impersonation, the scammer adds valuable details that can elevate the scam," says Hummel. "AI scammers are simply tapping into everyday technology available online – all they need is some of your own data to make quite a good impression of you," he explains. "However, for fakes to be truly believable, you need both a high quantity and quality of data – and currently, the abundance of data is low in quality," continues Hummel.

Banks and their customers should be more concerned about the details scammers seek and use to make their fakes more believable. "Criminals can use quality data – such as address, mother's maiden name, date of birth – to enhance their scams," explains Hummel. "These are details banks currently use for their security checks, and consumers are often giving this information – and more, such as fingerprints and photos – away without realising the risks. It only takes one good hacker to gain access to the cloud, where this data is stored, and impersonate you," he continues.

Fight fire with fire

In terms of deepfake scams, the biggest challenge facing banks is their difficulty in recognising the real voices of their individual customers. "Only real people can do that," argues Dörfler. "Banks have to commit to an expensive race. They need the latest detectors as a minimum wall of defence. However, AI scammers will also be

in that race. Sometimes the industry will be ahead, sometimes the criminals will be ahead. While banks' efforts may not provide a robust solution, doing something is better than doing nothing," he explains.

Hummel argues that technological solutions are a bank's best bet. "While banks have very basic technological means of defence, such as two-factor authentication, there are more advanced options available nowadays, like 360-facial recognition scans or face-to-face video checks.

"We are currently in the middle of an AI storm. It hasn't been around for that long, is developing quickly, and needs to be harnessed in a way that's safe to do so."

Christian Garcia,
CEO, Trusted Novus Bank

"Traditional banks seem to be lagging behind FinTechs, which are swift in their adoption of new fraud-prevention technology. For example, high-street banks still rely on sort code and bank account numbers. The problem with this data is its relevancy and availability to criminals, if you lose your card or phone. Meanwhile, digital-native competitors are using QR payments or single-use cards. This data, though readily available, quickly becomes irrelevant," adds Hummel.

Dörfler agrees that the commitment to technology is key. "For banks, the technology required to tackle the threat from technology itself is a money-consuming race in which there is no choice but to partake," he says.

Transactions are also happening so fast that scams can easily go unchecked. "Payments are almost instant, so it may be difficult for customers to recall transactions," says Hummel. "This creates a sense of urgency in mitigation practices, which could include AI tools that filter out unusual transactions. Pre-emptively, it could block anything suspicious and then wait for the bank to confirm the validity of the transaction with the customer."

Trust in intuition, urge caution

The vulnerability of human nature shapes our propensity to fall victim to criminal exploitation. Scammers pray on people's desires and emotions and on our brains that are wired to solve puzzles and find solutions. However, banks can leverage people's intuition. Our basic instinct is an internal repository of wisdom gained, lessons learnt and memories made, offering us invaluable insights without the need for conscious cognitive dialogue.

"If something feels off, then it probably is. Learning how to trust these feelings is key," advises Dörfler. "I believe that empowering our human intuition will become one of the most important security measures against AI fraud."

Inconveniently, the impetus falls on everyday individuals to figure out friend from foe. "While doubt puts people on high alert, they must rely on simple actions, such as checking the details of the message and verifying the identity of the sender – however believable both may be," he advises.

Hummel argues for the need of a collaboration entity between banks, governments and educational institutions. "People must be made aware of what AI can do and how we can develop and safeguard against its criminal activities," he says. Personalised campaigns that speak to individuals across the generations could help get the message across. "Reaching people to warn them about what AI can already do with their data, that's already available online, could help them become more cautious," he adds.

Garcia agrees that education and awareness are key. "We're learning all the time and have to keep abreast of the risks. Take social media, for example. Many fraudsters use it to learn about their potential victims, so we need to be more careful when socialising online."

TACKLING AI SCAMMERS

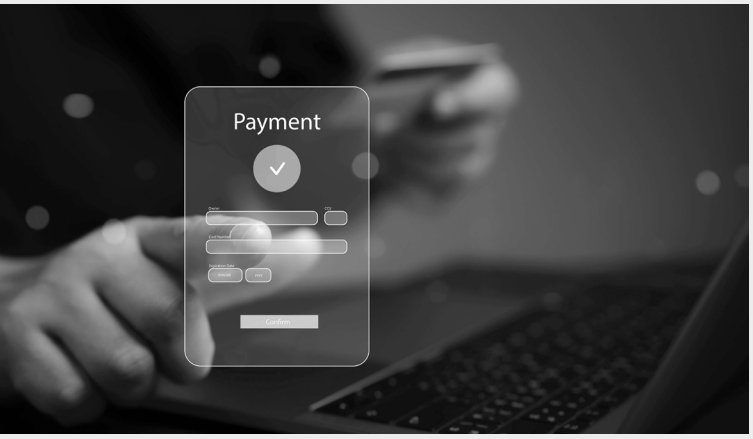
English is the reluctant language of crime

The prevalence of AI scams targeting customers within the UK banking sector could be down to the global use of the English language. "Many of the world's banks are British or, at least, English-speaking. For many multinational businesses, it's the main working language, so it all adds up," says Dörfler. "I think it's also equally important that the English language is far better processed than any other language, with an abundance of voice recordings. So, generating spoken text in English is far easier," he explains.

Hummel agrees on AI's proficiency of the English language. "English is the lingua franca of AI. Most of the training occurs in English because of the vast quantity of data available," he says.

However, Garcia believes that the prevalence of the English language doesn't need material attention when addressing the risks of AI. "English is widely spoken, yes, but it's not the only language. Asian languages cover a huge population and geographic scope. Many cybersecurity threats have originated in Eastern Europe and further afield."

Scammers may use the English language to their advantage, but customers can rely on their intuition. "Banks say that they will never ask you for your pin over the phone – and they don't. Customers require a degree of discipline. Criminals who deploy deepfakes rely on catching their victims off guard. After all, why would you have your guard up when you hear a familiar voice? Changing this is not necessarily a good thing – no one wants to have their guard up when among friends. However, more awareness can be useful," warns Dörfler.



Don't blame the tech itself

From data bias and privacy to transparency and accountability, AI cannot escape the pressing question of ethics. However, should the worker blame their tools? "AI does not actually have an ethics problem. Ethical issues derive from human beings and not computers. AI may make ethical issues more visible, but they are not tied to the technology itself."

While new generations emerging from digital-native environs may appear more technology-smart, and better able to spot deception, awareness shouldn't be a given. "The point is that people who aren't criminals don't think like criminals and find it very difficult to do so. Though it may not be our natural way of thinking, we need to be told that fraud can be committed – and by people who want to do harm," says Dörfler.

> **"For banks, the technology required to tackle the threat from technology is a money-consuming race in which there is no choice but to partake."**
>
> Viktor Dörfler,
> Professor of AI Strategy,
> University of Strathclyde

Hummel wonders whether an AI version of a human accountant could be an alternatively viable line of defence. Major B2B transactions typically evade fraud because there is usually an accountant acting as a conduit to ensure legitimacy. "An accountant builds that credibility that we all take for granted in our everyday transactions," he says.

Regulation has often been needed to engender ethical practices in business. "There's already discussion whether AI should be regulated across the board, or simply overseen by financial regulation. Either way, there is still much work to do," observes Garcia. "We need to collaborate between constituents of the sector, with continuous monitoring and auditing to detect biases and errors in AI systems, to ensure transparency and honesty about the ongoing risks," he urges.

The 'Wars of the AIs'

FIs cannot tackle scams on an individual basis, but they can urge caution and vigilance. However, banks can begin leveraging certain detection tools, which are constantly evolving, to help tackle fraud collectively. "The same people who are building the AI tools that can create deepfake are also making the best tools to detect those deepfakes," explains Dörfler.

Hummel argues that AI has become bifurcate. "We are seeing the 'Wars of the AIs' play out, with well-intentioned AI battling malicious AI," he explains. While players on either side look to outmanoeuvre the other, banks that invest in data-security technology can sharpen their competitive edge. "With AI, banks are usually behind the eight ball. They need to constantly innovate to overtake scammers and beat them at their own game," says Hummel.

Garcia points out that whenever there is business to be done, there will be interested parties. "Banks must ensure that the security technology they use cannot be overridden by AI technology, especially when in the wrong hands. Software security providers will be very interested, working full steam ahead in improving tools. Just like the boom of antivirus software, there will be businesses wholly focusing on AI protective software."

AI will enable banks to better identify AI fraud and scams, reducing the workload of professionals who can focus on more complex cases. Dörfler believes that standardisation at global level will have an important part to play, with ISO guidelines reinforcing the UK's regulatory landscape. "It's in all but the criminal's interest," he concludes. CB