FRAUD ■ OCTOBER 25 2023

Fraud detection and prevention: have automated tools gone too far?

Have financial institutions got the balance right between human and automated decision-making when it comes to fraud detection and management? Or are customer accounts being closed simply because a machine says no?

by Anita Hawser

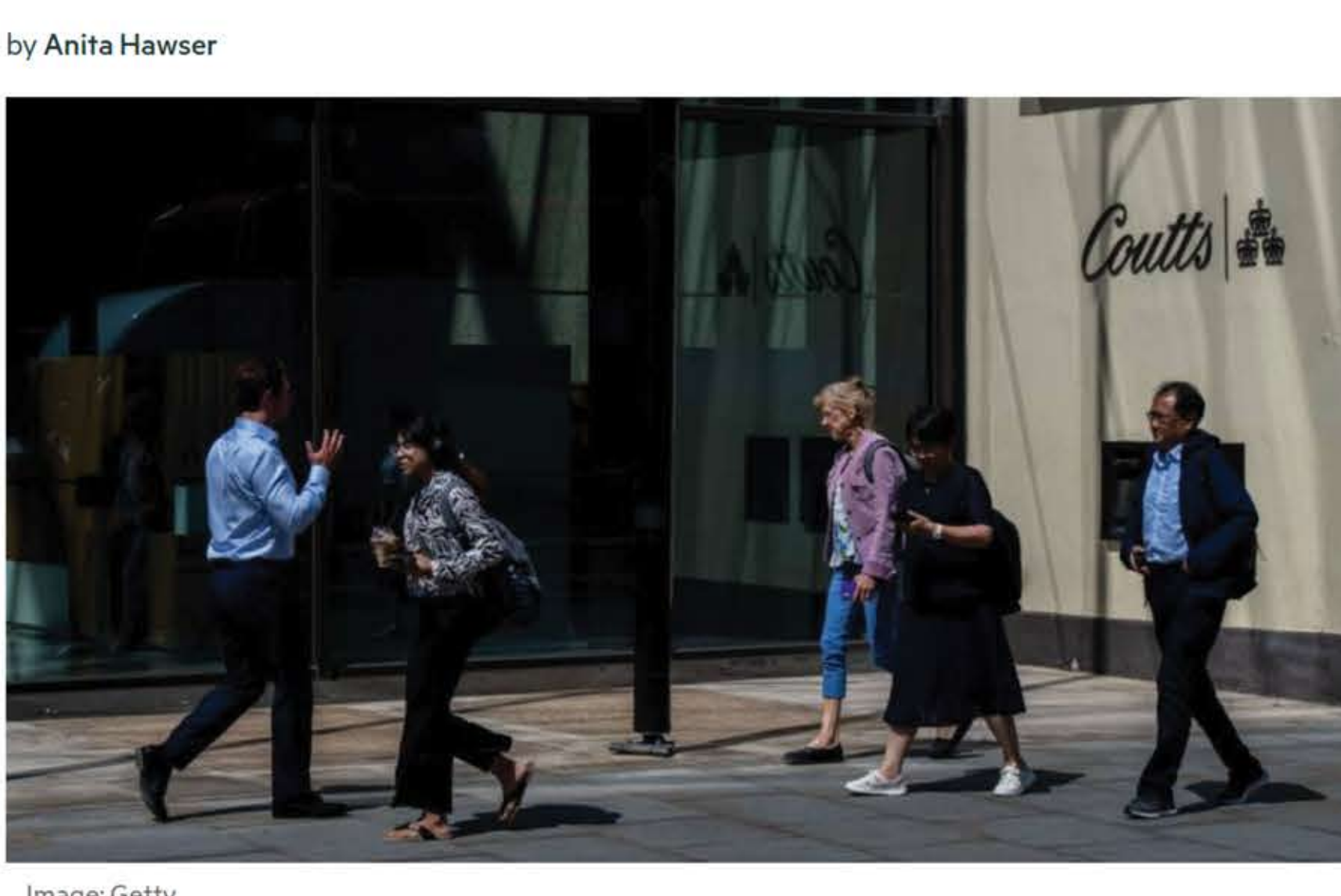

Image: Getty

Opening a bank account, making a payment or applying for a loan is relatively easy nowadays. Most of these financial services can be accessed via mobile or digital banking apps, which offer consumers convenience and speed.

But many customers are seemingly oblivious to the automated processes and decision-making that goes on behind the scenes to ensure that their financial lives online comply with anti-money laundering and preventing terrorist financing regulations.

To establish that the people or companies they are doing business with are legitimate and are facilitating legal transactions, financial institutions are ever more reliant on automated tools: transaction monitoring systems, automated fraud databases such as Credit Industry Fraud Awareness System (Cifas), as well as systems like SEON and Synetics Solutions for verifying and identifying customers and accounts, and artificial intelligence (AI) and machine learning for detecting complex patterns of behaviour potentially linked to fraud or criminal behaviour.

But is there a growing risk that financial institutions could rely too heavily on these automated tools and decision-making processes to decide what is an acceptable level of risk? Could it increase the likelihood of negative outcomes for the end customer, such as higher numbers of bank account closures or innocent people being accused of wrongdoing?

On the rise

Following the furore surrounding the closing of former UKIP leader Nigel Farage's account by private bank Coutts, which was linked to the bank's concerns about reputational risk, a freedom of information request by the UK's Mail on Sunday newspaper revealed that the number of account closures in the UK had skyrocketed, climbing to just over 343,000 in 2021-22. So far, this year, more than 200,000 business and retail bank accounts have been closed.

Debanking happens for a multitude of reasons: fraud, misuse, terrorist financing, money-laundering, inactivity, and mistaken identity. But Jeremy Asher, a consultancy regulatory lawyer at Setfords, who was one of the first lawyers to specialise in the removal of Cifas markers loaded by UK banks and other financial institutions against individuals, says he receives hundreds of enquiries a month from people from all walks of life who have been debanked as a result of a fraud marker (or, in some cases, multiple fraud markers) being loaded against them. In most cases, the customer is unaware a fraud marker has been applied until their bank account is suddenly closed or they are refused a particular financial product.

Some of these markers can last for up to six years and take a huge toll on individuals, Mr Asher says. "Once a fraud marker has been loaded, the vast majority of the time, a house of cards starts to fall," he says. "They lose their entire lines of banking, and they can't get credit facilities. They can't even rent a house, or get a mortgage."

> Once a fraud marker has been loaded, the vast majority of the time, a house of cards starts to fall.
>
> **Jeremy Asher**

So what is behind the high number of account closures in the UK? More than 86,000 cases of fraudulent conduct were recorded in the first six months of 2023, a decline of 6% compared with the same period in 2022, according to Cifas. But Mr Asher believes there is the possibility of banks being overly risk averse and relying on a computer-generated decision, rather than looking at the wider picture.

"Many financial companies use automated processes. They see something wrong, they will reject and load a [fraud] marker without asking any questions," he says, adding that many of these cases are simply not investigated properly, because a lot of banks will not make contact with customers to find out what went wrong.

Buried in data

Databases like Cifas contain information regarding people suspected of committing a financial crime. Cifas says around 75% of cases reported to its database every year relate to identity (ID) fraud (277,000 ID fraud cases were recorded in 2022). All Cifas members report instances of fraudulent conduct against their organisation to the database, enabling other members to search against their data. But this process happens without most customers knowing, unless they are a fraud victim and protectively register a marker.

Phil Coole, money-laundering reporting officer and head of compliance at UK challenger OakNorth Bank, says when a new customer is onboarded their details are automatically searched against databases like Cifas. "That's built into the terms and conditions," he explains. "It's not just protecting the bank, but also the wider economic climate and environment."

When reviewing matches against the data, Cifas says members must ensure that it is interpreted in a proportional manner according to their own risk appetite and the product being assessed. According to Cifas's standard of proof, there must be reasonable grounds to believe a fraud or financial crime has been committed or attempted, and evidence must be "clear, relevant and rigorous".

However, Mr Asher says Cifas recently reduced the standard of proof from a criminal to a civil one. In cases he represents, banks typically say they have looked at their processes and do not feel they have done anything wrong when loading a fraud marker against a customer. "But most banks only have 20 minutes to make a decision, and given the huge number of transactions they need to sift through, it is obvious that mistakes will happen," he says.

It is the decision-making process before a bank applies a fraud marker, in which transactions are monitored in real time using automated solutions, where things potentially go wrong, says Mr Asher. But whatever tools members use as part of their investigation processes, Cifas says they must investigate a match and reach the required Cifas "standard of proof" before recording a marker.

Yet a quick search of the UK Financial Ombudsman Service's website reveals hundreds of cases spanning a number of years of financial institutions' decision to load a fraud marker being overturned by the ombudsman. Often the reason given for overturning the marker is that it was not fair or reasonably applied.

Cifas maintains that the cases overturned by the ombudsman are extremely low compared to the 409,000 cases recorded by its members last year, and says it operates a clear complaints process, which is simple to access and allows consumers to raise a dispute without having to go down the legal route.

Gone too far?

But have we reached a tipping point where the increased use of automated tools and AI in fraud management and combatting financial crime is causing more people — including those who are innocent or victims of fraud — to be debanked? "That would be a really dangerous place to get to if computers were just making decisions for us on what is effectively someone's bank account or livelihood," says Mr Coole. "I'm not there yet, personally, and I'd be surprised if other people in my position are in other banks."

Automated databases such as Cifas require human intervention, he says, because their output generates a lot of noise. "The resulting noise has to be dealt with by a person right now," he says. "But I do know that to speed up the customer onboarding process, banks are trying to work towards a place, and possibly some are doing it already, where the technology can make certain decisions on its own. If I was in a bank doing that, I'd want to set it at a level that minimises customer impact and harm as much as possible so that it was only making really obvious decisions."

Mr Coole adds that there are no areas relating to financial crime decisions within OakNorth in which a computer makes a decision about a customer on its own. "However, I would imagine that some of our peers that have a greater scale of retail exposure are probably doing that, particularly where they are fintech-based or built out of a fintech-style institution," he says. "There's nothing inherently wrong with that, because there's a cost attached to a lot of this work and they're trying to use a computer or machine learning or AI to make appropriate decisions."

Mr Asher says he sees a lot of cases involving challenger banks loading fraud markers incorrectly, and believes there is insufficient human involvement in a lot of these organisations. He cites one example in which a bank recognised that a client had been hacked and did not load a fraud marker against them, while a smaller challenger bank refused to remove the marker. "There is this disconnect which suggests that the bigger banks have put in the proper tools, while challenger banks don't have as large fraud teams," he says.

The right balance

One UK challenger bank contacted by *The Banker* said it is perfectly clear on the reasons why a transaction is flagged or an account is closed, which it takes very seriously. Others contacted declined to comment.

Iain Armstrong, a regulatory affairs practice lead at regtech company ComplyAdvantage, says the decision to decline a prospective customer or to offboard an existing one is not taken lightly, particularly for challenger banks that are under considerable pressure to increase their customer base. However, there is the potential for these automated tools to be misused, he adds. "It's really about the interplay of your human capital with your technology, and like most things, it's about [getting the right] balance."

A report published in May by rating agency DBRS Morningstar says a fast onboarding process at challenger banks may result in a lack of sufficient information about the customer, and therefore a poor assessment of the customer's risk profile. A review conducted by the UK's Financial Conduct Authority in 2021 covering six challenger retail banks with more than eight million customers identified failures to gather sufficient information about customer income and occupation at the account opening stage, as well as limitations in organisations' financial crime risk assessment frameworks.

It is difficult to know whether these limitations can be linked directly to an overreliance on automated tools or decision-making. But Mr Asher insists that automated fraud systems and databases are unfair and too indiscriminate. He points to cases of fraud involving 'money mules', where young people on social media are lured into using their accounts to receive criminal or fraudulent funds, which are then used to conduct scams, commit wider fraud and other serious crimes, including people-trafficking.

Cifas's August 2023 Fraudscape report says "misuse of facility" accounts for nearly a fifth of fraud cases, with more than 17,000 cases having intelligence indicative of money mule activity, mostly using personal bank accounts. But Mr Asher says there is a difference between people who are complicit and those who are non-complicit, and automated fraud solutions are unlikely to make that distinction.

Enhanced accuracy

Sian Townson, a global expert in AI risk and ethics at Oliver Wyman, says preventing fraudulent activity without negatively affecting existing customers is a problem that existed long before AI was introduced. "From my perspective, AI has only enhanced accuracy," she says.

It has also taken mundane tasks away from humans. "When it comes to reviewing transactions, you want the human to work a lot more efficiently and focus their time where they add value," she adds.

Will AI replace people in fraud or financial crime teams? Ms Townson says there is a misunderstanding around how much of a decision the technology actually takes, as opposed to merely highlighting suspicious activity for human investigation. "We don't want a situation in which someone's disadvantaged because a machine says no, but equally, we don't want to be in the position where somebody's lost their life savings because we didn't detect fraudulent activity," she says.

> Banks need strong board-level leadership, to ensure they're meeting their own standards.
>
> **Sian Townson**

"Having an algorithm that monitors something in real time and sets off an alarm quickly is worth a lot, whether that's protecting your life savings, spotting indicators for money-laundering or the complex, interacting patterns that might suggest human trafficking."

To get the most from AI, Ms Townson says everyone, including the boards of banks, will need to upskill. "Whether or not the performance and ethics of the AI is good enough is a large ask of a board that hasn't necessarily come into their role as AI experts," she says. "Banks need strong board-level leadership, to ensure they're meeting their own standards and that they've got the right policies."

Provided firms have a good handle on their data and put these tools through proper assurance processes to ensure they are working as intended, Mr Armstrong says there is no reason why the use of automation and machine learning should increase the likelihood of an innocent consumer being wrongly excluded from a financial product.

Regulatory considerations

The greater onus being placed on banks to protect customers and ensure good outcomes for them — enshrined in regulations such as the UK's new Consumer Duty — could also see the use of highly automated tools and AI in fraud detection and financial crime management receive closer regulatory scrutiny.

"We've all got a very keen eye on what the first institution of issue is going to look like with Consumer Duty, and whether that has any interplay with derisking or any financial crime-related issues," says Mr Coole.

Only time will tell on which side of the debate the regulators fall. Meanwhile, in the wake of the Farage case, a recent Financial Conduct Authority (FCA) investigation concluded that no firm — banks, building societies and payment companies — closed an account between July 2022 and June 2023 primarily because of a customer's political views.

However, the FCA says further work is needed for it to be sure. "As we undertake that work, the time is also right for a debate on how we balance access to bank accounts with the threat of financial crime, as well as firms' reasonable risk and commercial appetites," the FCA stated.