FStech

ENTRUST

Financial Services Roundtable



FIGHTING ACCOUNT TAKEOVER IN THE AI ERA:

Rethinking identity, trust and customer protection

ENTRUST

At a roundtable hosted by FStech and Entrust (formerly Onfido) in Central London, senior financial leaders across fraud, risk, identity, digital banking, and customer experience discussed how their organisations are tackling account takeover fraud in the era of AI without compromising customer experience.

This special report details the key discussions at the event. Topics ranged from the most pressing threats faced by financial services organisations to the role of regulation in orchestrating the fight back.

Introduction

Account takeover has become one of the most pressing fraud challenges facing financial institutions. As cybercriminals supplement stolen credentials and social engineering techniques with AI deepfakes and automated attacks, leaders must ensure they can tell the difference between legitimate digital activity and the next attack.

At the same time, financial institutions must stay ahead of the curve or risk losing customers to more innovative competitors. Maintaining this balance requires a cross-departmental approach, combining customer outreach and a clear understanding of regulation with the latest threat data.



The trends putting pressure on security teams

The discussion opened with a brief speech by Minh Nguyen, vice president of product at Entrust. He explained how fraud has evolved over time and the unique sophistication of AI-powered fraud attacks.

Nguyen said that when he started working with the financial services sector on identification, anti-money laundering (AML) and identity security a decade ago, most interactions were hybrid.

This meant institutions knew their customers and interacted with them in person, with physical interaction forming the foundation of trust. This changed over the pandemic, he said, with trust becoming remote by default.

"The stage that we see now is not only are interactions remote, but the question of trust is pushed into its next tier: how do I trust people and that I'm actually talking to people in the age of AI and agents?" he said.

Fraud has changed to match, Nguyen explained, having shifted from a focus on faking documentation to Photoshopped documents and now deepfake-based attacks. Over the last few years, his team has tracked a 40 per cent increase in attackers injecting high-quality deepfakes into verification systems, known as injection attacks.

User expectations have also shifted, Nguyen added, with high demand for immediate payments that are as frictionless as unlocking one's phone. This pressure is coming from consumers and businesses, with Nguyen giving the example of remote workers wanting easy access to their work files without having to enter passwords repeatedly.

Finally, Nguyen said, the regulatory landscape is shifting all the time, such as new AML regulation and eIDAS 2.0 from the European Union.

"I see a convergence in discussions for us as practitioners," Nguyen said, adding that identity verification, know your customer, account opening and identity and access management teams are now sitting together rather than spread across IT, FinCrime and onboarding flows.

He challenged attendees to consider how to tackle the evolving fraud landscape with AI, balancing real risks and consumer expectations while adapting processes to incoming regulatory changes.



How AI is changing account takeover

A senior compliance figure at a British payments firm said that account takeover knows no barriers across age, wealth, intelligence, race, or background. One of their peers, a senior leader in fraud who also works in the British payments ecosystem, agreed, noting that AI is making account takeover easier for fraudsters to accomplish.

"Where previously fraudsters would have to do a lot more work to do account takeover, they're having to do less take because they can utilise AI, so the volume of the threat is going up," they said.

Around the room, leaders agreed that attackers are using AI to increase the pace and scale of existing attacks. A senior leader in risk at a British business bank said that as AI improves the sophistication of fraud, their organisation is investing in AI countermeasures.

"It's almost becoming militaristic," they said. "It's measure and countermeasure, we're hiring people to be AI defenders, as it were. And it's not going to go away."

One of the strongest layers of defence is still customer education, explained a fraud expert at a savings bank. They said that financial services organisations need to continue to provide a human touch alongside their resources on fraud to help customers fully understand why fraud occurs and ensure it doesn't happen again.

A head of fraud prevention and financial crime at an asset management company echoed this, noting that their firm is focused on providing customers with fraud education. They added that internal conversations between infosec, business and financial crime teams is needed, seconding Nguyen's observation that cross-departmental collaboration is key.

For years, AI fraud has been defined by social engineering and phishing because initial large language models were optimised for text rather than multimodal outputs. But around the room, attendees made clear that deepfakes and voice clones are now being used for impersonation-fuelled account takeover attacks.

An expert in digital assets and FinTech at a UK investment bank said that they have been startled by AI tools that can replicate a person's voice based on just 15 seconds of audio. Firms such as ElevenLabs have guardrails to stop users from leveraging this for malicious purposes but open-source Chinese models do not, they warned.

"I speak a few languages, so I turned it around into Russian," they said. "It was able to speak like me, with the Russian accent as I speak. I was baffled by that."

These sophisticated attacks are not yet ubiquitous, said the head of financial crime at a British business bank. They noted that "old school" social engineering remains common, with AI-driven attacks still in the minority.

However, they added, fraudsters are evidently using AI to assist them with more traditional fraud vectors such as phone calls and to generate realistic web pages from reputable organisations such as the Financial Conduct Authority.

An economic crime analytics expert at a national UK bank said that they are also concerned by AI-fuelled authorised push payment (APP) fraud, where customers are convinced by attackers to send money into fraudulent accounts on a false premise. Across both APP and account takeover, they said, their organisation is looking to see where AI can be used to flag impersonation and warn customers when they are at risk.

"We're trying our best to use the technology to overcome it but, as people mentioned, criminals don't have restrictions on what they can do whereas banks and other institutions do."

Overlooked risks and demand for convenience

The discussion moved on to consider parts of the customer journey that financial institutions may overlook, as well as those that may form particular points of weakness.

One senior fraud leader at a payments firm said that organisations can focus too much on targeting support to the most vulnerable customers, when AI in fact puts all customers equally at risk.

"I believe in monitoring the vulnerable customers, but I think it can also make us very tunnel visioned and

narrow minded," they said. "I think we don't encapsulate the fact that everyone can potentially become a victim to AI fraud."

The response, they said, must be controls that are cross-sector and aim to protect all customers.

Several attendees agreed that customers can overestimate how resilient they may be to fraud and stressed that leaders should not fall into this trap. People who frequently use AI may abe more vulnerable to AI fraud, rather than less, suggested a digital assets and expert at a UK investment bank.

"For example, I have given permission to read, write and send emails to my personal account to a few AI models," they said.

"I know what I'm getting into," they added, while noting that AI agents sold under the promise of automating the bureaucracy of everyday life are a powerful lure that could be vulnerable to targeted fraud.

This returned the discussion to another point first outlined by Nguyen: the increased demand for low-latency, streamlined customer processes.

"Immediate gratification is not quick enough," warned an expert in operational risk at a British business bank, noting that the financial services sector needs to strike a balance between immediacy and safety.

"People are used to looking at their phones and tapping away without necessarily taking into consideration the consequences of their actions."

For one attendee, an expert in anti-corruption and fraud prevention at a multinational asset management company, the answer is more government involvement.

"There needs to be more regulation and convergence on privacy, AI regulations, and how the financial services industry should adapt to it," they said.

As an example of the kind of problems today's instant gratification systems enable, they cited cases of North Korean workers being inadvertently hired for remote positions at major institutions. The guardrails to prevent this need to be set out in the public sector, they added, much like the current conversations around banning social media for under-18s.

A senior leader in fraud at a payments firm seconded this proposal, noting that clear legislation and education on identifying AI content is needed not only for today's workers but also its children.





Is friction a bitter pill?

As AI takes increasing advantage of streamlined online systems, financial services organisations are under growing pressure to fight fraud not only at scale, but speed. The attendees turned to the problem of introducing security checks without damaging the customer experience.

An economic crime expert at a High Street UK bank said the aim should be to create systems that are "reassuringly slow," noting there may also need to be a pushback against algorithms that encourage users to do every task quickly.

The struggle, explained an expert in compliance at a payments firm, is that this speed is being driven by supply and demand. If organisations ease off delivering on this low-latency experience, they said, competitors will beat them to it. They added that for this reason, they do not think legislation can tackle the problem alone.

Greater consumer responsibility is ultimately needed, argued the head of financial crime at business bank.

"I think there needs to be a little bit of consumer heartache and they need to take responsibility," they said. "There is a little bit of thinking across the population that, 'Oh, your bank will refund you, don't worry', and actually that can't be the answer."

The introduction of additional security checks can also raise the risk of incorrectly flagging legitimate activity as fraud. Attendees stressed that this is where messaging and communication is key.

A risk leader at a UK bank said that their call centre workers are trained to explain to customers that any frozen payments or additional checks are for their benefit, and to escalate payments of a higher monetary value where possible.

At the same time, financial institutions must be

vigilant and check that seemingly disgruntled customers are who they say they are. The head of financial crime at a UK bank said they have dealt with cases in which fraudsters bombard fraud teams with complaints in an attempt to make them second guess their defensive decisions.

For now, threat actors can generally be verified from specific tells, they explained: "If you've got somebody genuine, they tend to say, 'Why have you blocked my account? I need to do payroll' or 'I need to pay my bills'. Whereas I've found the bad guys tend to say, 'I assume you've blocked my account because you have submitted a report and are holding my funds under this regulation'."

Several attendees said that sticking to intuition and reassuring customers over any anti-fraud action is a clear case for keeping humans in fraud teams, rather than replacing them with agents.

This was summarised by a senior fraud expert at a UK payments firm: "We find a lot of times where there's peer pressure to unblock an account […] sometimes you need that underlying staff member to follow their gut and be adamant to not do it."

Areas of improvement

Looking ahead, all attendees agreed that the financial services industry needs to greatly improve on collaboration and information sharing. Suggestions included the creation of more formal sharing arrangements between incumbent banks and neobanks, FinTechs and other digital challengers.

"There's no one conglomerate for it," said a fraud expert at a national payments firm. "We have to follow what the big banks do because they're the ones setting the tone".

The head of financial crime at an asset management company agreed, noting it is still considered "taboo" to share insider threat data even though it is extremely useful for preventing financial crime. There is a role in this field for AI-powered internal monitoring, they added.

More guardrails may also be needed, but a FinTech expert at an investment bank warned that a balance is required.

"At what point do you have so many guardrails that it takes two times as long as it otherwise would have taken to get the process done?" they asked. "On the other hand, if you don't have enough guardrails, you have bad actors coming through."

The head of financial crime at a UK bank said consumer choice is key, but only if bundled with education. They gave the example of FinTechs now enabling customers to delay payments to allow time for consideration.

"That choice needs to be in consumers' hands," they said. "Either I want an immediate, frictionless service and I take the risk that comes with that, or I'm happy to slow things down and have these guardrails in place."



Conclusion

Throughout the discussion, attendees outlined some of the key challenges that AI poses in defending against account takeover fraud.

Financial services organisations are grappling with both a technological and cultural change. AI is speeding up operations and driving new risk vectors at the same time as customers are demanding less friction and more seamless user experiences.

Summarising the conversation, Nguyen said that it is clear AI can be used both for good and bad outcomes. He pointed to new technologies such as agentic commerce being met with both enthusiasm and distrust, and multi-layered AI attacks driving more sophisticated account takeover fraud.

He also encouraged attendees to engage in more cross-sector information sharing. He added that information shared by Entrust and by FinTechs can be greatly supplemented by data from large financial institutions.

As established threat management techniques are upended by changing technology, financial services organisations face a great deal of uncertainty.

While their customers flock to the latest tools and user experiences, these critical firms must work to integrate the right level of checks and balances to ward off increasingly sophisticated social engineering and impersonation.