FIGHTING FRAUD:

The Threat and Promise of Generative AI

BANKING DIVE

Custom content for Mastercard by studioID

The digital world is full of dichotomies, especially when it comes to protecting your institution from financial fraud. On one hand, the democratization of computing power has helped banks create convenient and secure online banking solutions — expanding products and the customer market. But on the flipside, technology has also made it easier and faster to commit fraud.

"Technology has not only made it possible for more people to commit fraud but also to scale fraud to an enterprise level," says Ian Li, Director of Enterprise Sales for Mastercard Identity. In fact, Nasdaq reported that fraud scams and bank fraud schemes caused $485.6 billion in global losses last year.

The rise of generative AI presents similar opportunities and risks. In an economic landscape marred by growing credit card debt and negative economic sentiment from consumers, generative AI can turn an interest in committing fraud into a full-blown campaign. Yet, while AI presents a threat, it may also be a solution, improving the fight against fraud and even helping drive growth, according to David Britton, Vice President of Global Identity and Fraud at Experian.

"Experian is a big proponent of leveraging the same insights that are effective in fraud prevention to also improve business growth," Britton says. "Generative AI can help create unique insights that will enhance fraud detection while helping companies understand their legitimate customers that much better."

READ THIS PLAYBOOK TO LEARN MORE ABOUT:

1. The current fraud landscape and why traditional fraud solutions aren't enough

2. The rise of generative AI and the threat it poses

3. How machine learning and dynamic data helps banks fight back and improves the customer experience

FINANCIAL CRIME TAKES A TOLL

$3.1T

Illicit funds that flowed through the financial system in 2023

$485.6B

Fraud losses reported worldwide

Source: Nasdaq

Generative AI ups the ante

Financial institutions are beginning to grasp that traditional KYC efforts aren't enough to prevent fraud. "Organizations are doing so much, and yet fraud persists," Li says. "Now, with generative AI in the picture, it can happen at a speed and scale that wasn't even possible a few years ago."

Generative AI has the potential to accelerate financial crime at an exponential rate. The increased computing power introduces a host of new fraud risks, including:

1. Scaling synthetic identity creation
2. Manipulating images, videos and voices.
3. Creating fraudulent documents.

1. Scaling synthetic identity creation.

Until very recently, automating the process of stitching together identities or trying to pass the security measures of a bank required highly skilled programming knowledge. However, generative AI gives experienced and less technically savvy criminals access to programs that make and automate synthetic identities. "These programs enable anyone to scale fraud attacks and brute force their way past signup attempts," Li says.

For example, generative AI allows scammers to create and try an infinite number of ID combinations until they find one that works. The technology also helps fraudsters identify vulnerabilities more quickly, which opens the doors to even more fraud attacks. "The concern is that the AI lets fraudsters operate at a speed and scale that puts banks on their heels," Li says. "They can't respond to the scope of the attack."

2. Manipulating images, videos and voices.

Many organizations ask customers to perform biometric tests to authenticate their identity further. This can include snapping a photo with a driver's license, recording a voice message or taking a video. As Britton explains, "If I'm a fraud fighter, I'm looking for proof of life." But how do you know if these images are authentic in a generative AI era? Scammers already use generative AI to create lifelike images, videos and even voices. The National Law Review recently reported that a deepfake video featuring an AI version of a Hong Kong bank's CFO convinced a bank branch manager to transfer $25 million into fraudulent accounts.

> "If I'm a fraud fighter, I'm looking for proof of life."
>
> **DAVID BRITTON, VICE PRESIDENT OF GLOBAL IDENTITY AND FRAUD, EXPERIAN**

3. Creating fraudulent documents.

The ability to create undetectable fraudulent documents — and a lot of them — is another looming threat. As noted, KYC efforts often rely on documents to validate a customer's identity. However, fraudsters now leverage advanced technology to produce documents indistinguishable from genuine ones. And they are doing so on a massive scale. The situation becomes even more tenuous as criminals tap into the power of machine learning to create deep fake backgrounds that support fraudulent documents. Scammers could create fake social media accounts with fake photos and life milestones, dripping out information over time. With this long game, traditional KYC goes out the window.

The evolution of technology continues to provide new tools and methods that scammers can use to improve the quality of their fraud — and the scope of their efforts. "These are highly creative, motivated and well-funded individuals and organizations that don't have to abide by regulation and aren't constrained by a budget," Britton says. "It's an arms race and it's only accelerated over time."

FRAUD ON THE RISE

43%

Financial institutions that reported an increase in fraud in 2023 compared to 2022

65%

Average amount that the cost of fraud increased in 2023

Source: PYMNTS

The data gap

Of course, financial institutions have been investing in fraud solutions and trying hard to keep pace with technology trends that help their cause. "The only way to fight more sophisticated fraud is with more sophisticated solutions," Li explains. Many financial institutions agree, with nearly 50% reporting that they already use AI and machine learning to fight fraud.

But even as organizations understand the importance of technology in this battle, many are still reliant on limited sources of data. The market is awash in compliance and KYC solutions that rely on static or deterministic data to ascertain whether a customer is legitimate. The latter is often called "first-person" data and refers to information organizations know to be true.

Some key examples of deterministic data include:

- Social security number or tax ID
- Home address
- Credit score or credit header
- Proof of identification such as driver's license
- Potential sanctions or OFAC list

SYNTHETIC IDENTITY IS A REAL PROBLEM

$3B

U.S. lender exposure to synthetic identities

Source: TransUnion

"Solutions like these have value and can provide specific information about customers," Li says. "But the problem is that they don't paint the whole picture." For example, customers may create fraudulent identity documents or use someone else's. Synthetic identity theft complicates the KYC picture, by providing some authentic aspects of real people's identity (in a Frankenstein form).

Legacy solutions that only rely on deterministic data struggle to verify synthetic identities. The scale at which generative AI can create them means that many organizations may become overpowered by a tidal wave of fraudulent accounts. Britton predicts this will be an ongoing issue.

"Fraudsters have become quite good at playing the long game," Britton says. "We're seeing a lot of accounts being created using synthetic identities — but the fraudsters don't plan to use the accounts now; instead, they are setting them up for future work."

> "The only way to fight more sophisticated fraud is with more sophisticated solutions."
>
> **IAN LI, DIRECTOR OF ENTERPRISE SALES, MASTERCARD IDENTITY**

Dynamic data makes the difference

Fortunately, there are innovative solutions available that financial institutions can use to tackle these next-generation risks. "The advent and progression of generative AI in the fraud prevention space is really exciting," Britton says. "There are a lot of opportunities for what companies can do to prevent fraud and benefit the business."

Many companies are exploring fraud solutions that utilize dynamic data and contextual insights, which provide a deeper understanding of the underlying risk of a person or transaction. Analyzing the dynamic data created by customers gives financial institutions a sense of a customer's entire digital footprint. For example, dynamic identity solutions aim to assess an individual's online identity elements, such as name, email, phone, address or IP address. These solutions also look at usage factors such as how often individuals transact, who they transact with and how long they use products, across which devices.

Instead of focusing only on who the person is, dynamic data-based solutions consider how they act and whether their behavior makes sense. For instance, why would an individual apply for a loan or a credit card with a phone number they've never used before? Or with an email account they just established yesterday? Or from an IP address 2,000 miles away from the state they say they live in?

"Unlike deterministic or static information, these dynamic signals can't be purchased and are much more difficult to manipulate," Li says. Using machine learning models, these solutions analyze massive datasets, identifying patterns of how regular customers behave and creating red flags for customers who don't meet those criteria.

"There's a network-based approach that allows you to analyze data across the entire industry," Li adds. "This enables companies to keep pace with fraudsters as they change their methods and update models to reflect the evolution of legitimate customers."

> "There are a lot of opportunities for what companies can do to prevent fraud and benefit the business."
>
> **DAVID BRITTON, VICE PRESIDENT OF GLOBAL IDENTITY AND FRAUD, EXPERIAN**

How Mastercard Identity helps

Mastercard Identity understands that the key to participating in and maximizing growth in this fast-evolving digital economy is a verified and trusted identity. Our AI-powered identity verification solution complements the KYC process, leveraging machine-learning-derived data that examines the customers' digital footprint and analyzes distinctive behavioral biometric patterns. Our probabilistic risk scores make it easier to not only identify customers with confidence, but also anticipate fraud trends.

With Mastercard Identity, you know:

- The difference between legitimate customers and suspicious ones
- What makes a trustworthy customer.

With Mastercard Identity, you know:

- **The difference between legitimate customers and suspicious ones.** We build our models to analyze and recognize normal and abnormal customer behavior (as well as the "normal" behavior of fraudsters). These models update in real time, meaning that they reflect the most current ways that actual and fraudulent customers are behaving.
- **What makes a trustworthy customer.** Trustworthy consumers typically have a long-standing history that is challenging to replicate, offering a heightened level of pre-KYC confidence. Our solution focuses on digital signals that cannot be purchased, such as email usage, history of IP addresses and the first time a phone and email were used together.

Fraud risk continues to evolve and increase, seemingly by the day. But so do the tools available to protect your organization and customers.

Connect with Mastercard Identity to learn more about how dynamic data signals can improve fraud detection and protect your organization from the growing threat of generative AI.

studio / ID

BY INDUSTRY DIVE