MIT Technology Review
Insights

Produced in partnership with

PLAID

As fraudsters up the ante with the help of AI tools, organizations need to build better defenses, data networks, and dialogues.

Battling next-gen financial fraud

From a cluster of call centers in Canada, a criminal network defrauded elderly victims in the US out of $21 million in total between 2021 and 2024. The fraudsters **used voice over internet protocol technology** to dupe victims into believing the calls came from their grandchildren in the US, customizing conversations using banks of personal data, including ages, addresses, and the estimated incomes of their victims.

The proliferation of large language models (LLMs) **has also made it possible to clone a voice** with nothing more than an hour of YouTube footage and an $11 subscription. And fraudsters are using such tools to create increasingly more sophisticated attacks to deceive victims with alarming success. But phone scams are just one way that bad actors are weaponizing technology to refine and scale attacks.

Synthetic identity fraud now costs banks $6 billion a year, **making it the fastest-growing financial crime in the US** Criminals are able to exploit personal data breaches to fabricate "Frankenstein IDs." Cheap credential-stuffing software can be used to test thousands of stolen credentials across multiple platforms in a matter of minutes. And text-to-speech tools powered by AI can bypass voice authentication systems with ease.

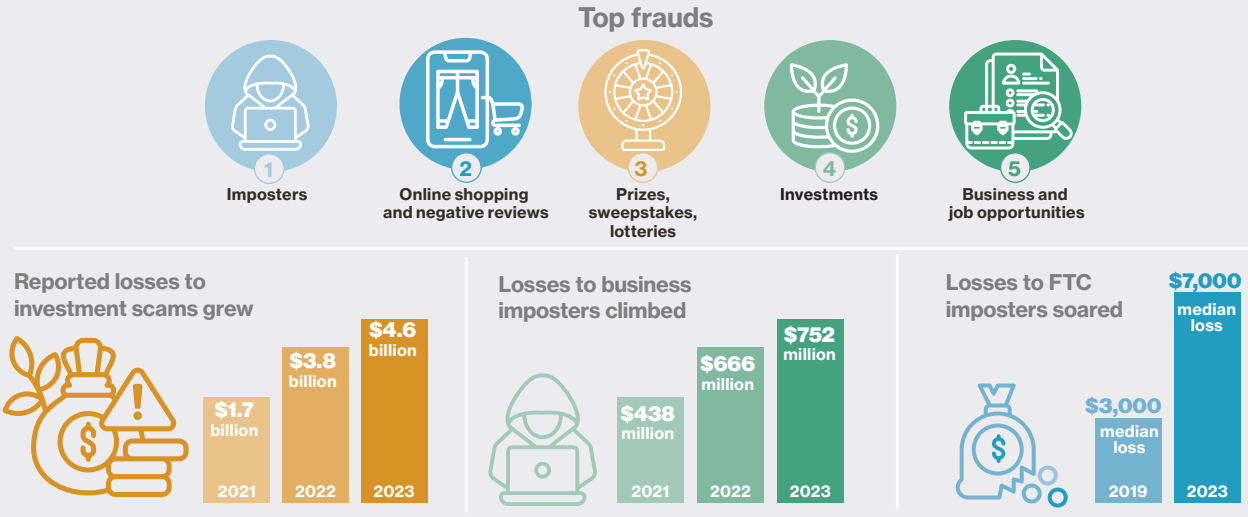
"Technology is both catalyzing and transformative," says John Pitts, head of industry relations and digital trust at Plaid. "Catalyzing in that it has accelerated and made more intense longstanding types of fraud. And transformative in that it has created windows for new, scaled-up types of fraud."

Fraudsters can use AI tools to multiply many times over the number of attack vectors – the entry points or pathways that attackers can use to infiltrate a network or system. In advance-fee scams, for instance, where fraudsters pose as benefactors gifting large sums in exchange for an upfront fee, scammers can use AI to identify victims at a far greater rate and at a much lower

Key takeaways

1. Financial fraud is on the rise as criminals leverage easily accessible tools like generative AI to vastly increase the scale and sophistication of attacks.
2. Traditional fraud-prevention tools are no longer adequate. Organizations need to invest in additional layers of AI-enabled security and use data sets unknown to fraudsters.
3. Participating in data-sharing networks across sectors and actively working to help shape policy responses will create a united front against fraud.

Figure 1: Imposter scams were the most common type of fraud in the US in 2023



Source: Compiled by MIT Technology Review Insights, with data from the FTC, 2025

"Technology is both catalyzing and transformative. Catalyzing in that it has accelerated and made more intense longstanding types of fraud. And transformative in that it has created windows for new, scaled-up types of fraud."

John Pitts, Head of Industry Relations and Digital Trust, Plaid

cost than ever before. They can then use AI tools to carry out tens of thousands, if not millions, of simultaneous digital conversations.

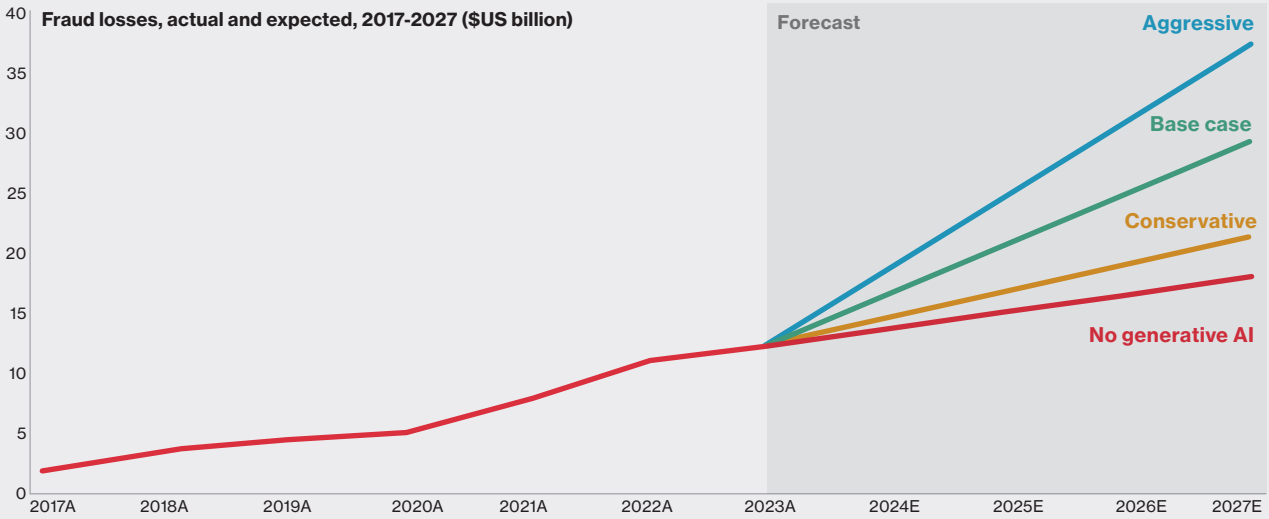
And the combined impact is fraud losses spiralling at unprecedented rates. In 2023, the US lost $12.3 billion to fraud. Generative AI is expected to make this figure surge, growing to as much as **$40 billion in losses by 2027**, according to estimates by Deloitte (see Figure 2).
For the financial services sector, that could spell crisis without proactive action, warns Pitts. "Fraud losses are increasing between 20% and 25% per year in financial services," he says. "From a pure dollars and cents perspective, you cannot sustain a 20% growth in fraud losses every year. Something's got to give. But from the reputational side, too, AI-enabled fraud is driving the ability to spoof trusted institutions as part of its execution. The ability of a fraudster to convincingly impersonate a government agency, your bank, or your credit card company is astronomically higher than it was even two years ago. It's a huge problem, reputationally."

Preparing for an AI arms race

Relying on traditional fraud prevention tools to keep up with these ever-evolving fraud tactics is tantamount to bringing "a stick to a gunfight," warns Pitts. Classic fraud detection zeroes in on transaction anomalies without access to wider contextual data. By moving between different platforms and accounts to legitimize payments, fraudsters can exploit this narrow viewpoint with ease.

Meanwhile, two-factor authentication – the prevailing security measure adopted by financial institutions in the last two decades – can be bypassed with a SIM swap and a benign call to a cell service provider. These methods lack depth and context, leaving institutions exposed to fraudsters who have, quite simply, a better toolkit to hand. It's perhaps not surprising, then, that **57% of financial**

Figure 2: Fraud losses are predicted to rapidly increase in the years ahead as a result of generative AI



A = actual E = estimated
Source: Compiled by MIT Technology Review Insights, based on data from Deloitte, 2025.

services organizations and 66% of lending organizations in North America reported an increase in overall fraud levels in the past 12 months.

Yet, there remains some reluctance to reevaluate and invest in building up better defenses, says Danica Kleint, product marketing manager for fraud solutions at Plaid. "A lot of companies are still using traditional methods of verification because risk teams tend to prefer what they are comfortable with and used to," she says. "As fraud tactics become more advanced, risk teams need to layer in signals that are resilient to spoofing – leveraging unique data sources that fraudsters haven't adapted to and are significantly harder to manipulate."

This begins with using the same technology fraudsters use to bolster defenses, says Pitts. "This is, to put it bluntly, an arms race," he says. "The fraudsters are deploying AI tools that give them new surfaces, new scale, and new cost reduction in how they commit fraud. If you are still relying on manual human driven processes for preventing that fraud, then you have absolutely lost that arms race."

Some leading organizations have already recognized this and taken action. **J.P. Morgan's fraud team has been using LLMs** for payment validation screening since 2021, for instance, resulting in a reduction in both fraud and false positives. The by-product has been a boost to user experience, too, with AI-enabled systems adding speed and reducing account validation rejection rates by 15% to 20%.

Wells Fargo has also embedded AI and machine learning (ML) into its fraud defense strategy. The financial services firm, which has around $1.9 trillion in assets, has layered ML models into its authentication systems to combat false positives. It has also deployed neural networks to identify patterns in customer accounts and detect fraud.

Such additional layers in fraud prevention need not require any trade-off with user experience, says Kleint. "It's about leveraging the data that we already have in a different way without adding additional burden to the consumer experience," she explains. For example, many organizations already ask new users to validate identities via a blend of biometric data – a selfie taken on their smartphone – and demographic data, such as their birth date. With AI, they can instantly detect a discrepancy between the two.

"We're not gathering any net new information, we're just analyzing what we already have in a different way," Kleint adds. "As you do those types of comparisons across many pieces of data, you start to get very effective prevention."

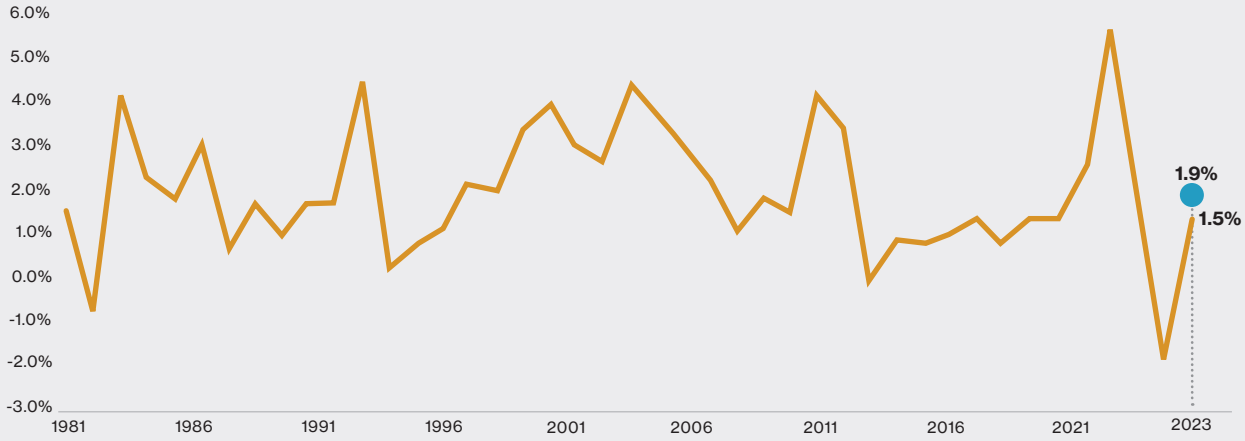
However, organizations need to also look beyond their own systems and technologies in order to develop robust fraud defense. Today, bad actors can access social media, telecoms, and even search engines to identify and initiate dialogue with unsuspecting victims, before switching between multiple accounts and payments platforms to distort suspicious activity.

"As fraud tactics become more advanced, risk teams need to layer in signals that are resilient to spoofing – leveraging unique data sources that fraudsters haven't adapted to and are significantly harder to manipulate."

Danica Kleint, Product Marketing Manager for Fraud Solutions, Plaid

Figure 3: US productivity growth would have been 0.4% higher in 2023 without fraud losses

This difference would put less inflationary pressure on an economy, resulting in slower price growth.



Source: Compiled by MIT Technology Review Insights, based on data from Nasdaq, 2025

Without incorporating network-based data for high-scale fraud signals alongside their internal fraud prevention measures, financial institutions can be blind to external threats, says Kleint. "But if you can have a sophisticated solution that includes multiple methods, building on top of each other, working together across the entire customer lifecycle, that's how you can prevent this next-gen fraud from happening on your platform," Kleint adds.

At Plaid, for example, its anti-fraud network consortium called **Beacon** adds layer by sharing real-time fraud insights across participating fintech companies and financial institutions – stopping the proliferation of fraud. In addition, the Beacon consortium provides deep insights into bank account risk, how your users are connected across your ecosystem and more.

"Fraud is everyone's problem to solve," says Pitts. "It's a collective team sport that we, the financial ecosystem, need to engage in together. If you are not pursuing a network-based defense where you are sharing information with lots of different companies, you are going to have disproportionate levels of fraud because there are limits to what you can do individually. The next wave of advances that we're going to see are from collective information sharing across different parties."

Collaboratively shaping the future of fraud

Private-public collaboration will also be instrumental in the fight against tech-enabled fraud. In the US, The Aspen Institute, a non-profit organization, is working to build an anti-fraud ecosystem with the Financial Security Program's National Task Force for Fraud & Scam Prevention, which launched in 2024. The multi-sector initiative brings together representatives from the US government, law enforcement, the private sector, and civil society organizations, each with a stake in the game.

"We have representation from all of those sector actors at the table, and we're talking through what needs to be done to prevent fraud and scams from harming consumers. Sharing information across these silos is a big piece of that puzzle," says Kate Griffin, director of the task force at the Aspen Institute Financial Security Program. "Questions being raised include how do we actually know what data each of us has that we could share? What are the best in class technologies we should use to share data while preserving privacy? And, how do we understand and mitigate any legal risks are are encountering?"

Long-term, the ambition is to develop a coordinated national strategy in the US that incorporates each element of this ecosystem. Such a strategy will broaden its scope far beyond individualized strategies at fintech companies and financial institutions to embrace a whole-of-ecosystem approach to fraud prevention. That may include equipping law enforcement officials with more advanced training and tools to combat AI-enabled fraudsters, suggests Griffin. It may see the introduction of a more robust legal framework to govern effective data-sharing.

Policy changes will be needed to help private sector players accelerate their own anti-fraud efforts, believes Pitts. There are three he sees as a priority. First, an amendment to the exemption for information sharing in the US Patriot Act to go beyond financial institutions. Second, the creation of a centralized anti-fraud function within government rather than the fragmentation across multiple enforcement agencies and jurisdictions that currently exists. And third, greater clarity on the tension between universal access to bank accounts and the exceptional cases where that access must be limited to remove bad actors.

To achieve these goals, Pitts says he'd like to see the US government adopt a firmer position when it comes to the shared responsibility to tackle rising rates of fraud. "I'd like to see a stronger mandate to make it clear that fraud is everyone's business and they need to be participating in these anti-fraud initiatives," he says. "Financial services is a trust and reputation business. If you erode that trust too much, it hurts everyone."

An evolving threat

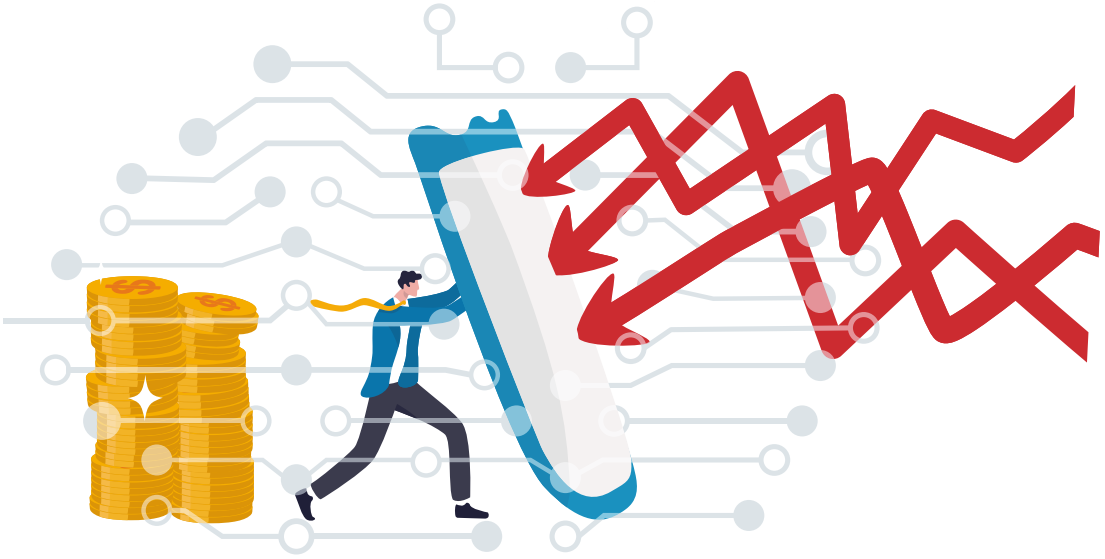
Both AI-enabled fraud – and the methods to combat it – are in their nascent stages. We all need to be prepared for the shape of the threat to morph and evolve as a result, as criminals find new ways to circumvent new layers of security.

The aim, therefore, is to limit and prevent damage, rather than destruction, says Griffin. "Our goal is to prevent there from being victims," she says. "As one of the task force members has said to me, "this work is not dragon-slaying. When you slay a dragon, the quest is over. Fraudsters are criminal actors that will keep innovating and trying to perpetrate crimes; we have to continue to evolve the fight to better deter criminal actors and starve the business model itself."

But the hope is that by utilizing advanced technology in a layered, defense-in-depth approach, proactively participating in cross-platform data consortiums and building a productive public-private dialogue, millions of those victims might still be spared.

"Fraud is a collective team sport that we, the financial ecosystem, need to engage in together. If you are not pursuing a network-based defense where you are sharing information with lots of different companies, you are going to have disproportionate levels of fraud."

John Pitts, Global Head of Industry Relations and Digital Trust, Plaid



"Battling next-gen financial fraud" is an executive briefing paper by MIT Technology Review Insights. Laurel Ruma was the editor of this report, and Nicola Crepaldi was the publisher. MIT Technology Review Insights has independently collected and reported on all findings contained in this paper. We would like to thank the sponsor, Plaid, as well as the following experts for their time and insights:

Kate Griffin, Director, National Task Force on Fraud and Scam Prevention, The Aspen Institute Financial Security Program

Danica Kleint, Product Marketing Manager for Fraud Solutions, Plaid

John Pitts, Head of Industry Relations and Digital Trust, Plaid

About MIT Technology Review Insights

MIT Technology Review Insights is the custom publishing division of MIT Technology Review, the world's longest-running technology magazine, backed by the world's foremost technology institution – producing live events and research on the leading technology and business challenges of the day. Insights conducts qualitative and quantitative research and analysis in the US and abroad and publishes a wide variety of content, including articles, reports, infographics, videos, and podcasts. This content was researched, designed, and written entirely by human writers, editors, analysts, and illustrators. This includes the writing of surveys and collection of data for surveys. AI tools that may have been used were limited to secondary production processes that passed thorough human review.

From the sponsor

Plaid is a data network that powers the fintech tools millions of people rely on to live a healthier financial life. We work with thousands of fintech companies like Venmo and SoFi, several of the Fortune 500, and many of the largest banks to make it easy for people to connect their financial accounts to the apps and services they want to use. Plaid's network covers 12,000 financial institutions across the US, Canada, UK and Europe. Headquartered in San Francisco, the company was founded in 2013 by Zach Perret and William Hockey.

PLAID

Illustrations
Cover art by Adobe Stock and spot art assembled by Chandra Tallman Design with art from The Noun Project and Adobe Stock.

MIT Technology Review Insights

www.technologyreview.com

insights@technologyreview.com