neuroID

A part of experian

WHITE PAPER • NOVEMBER 2024

The 2025 Fraud Defense Playbook

Industry Trends & Practical Tactics

Drawing on industry insights from the *Experian 2024 Identity and Fraud Report,* NeuroID's extensive attack data and our in-house fraud expertise, we've identified the top trends likely to shape the fraud landscape in 2025 and outlined strategies for fraud leaders to stay ahead.

Kudzu is an invasive climbing vine that haunts gardeners' nightmares. Dubbed "the vine that ate the South," it spreads across trees, power lines and buildings while suffocating entire ecosystems.[1] With roots that can reach 12 miles deep and weigh 300 pounds, Kudzu is nearly impossible to displace once it takes hold.[2]

Goats can't read those scary stats. But they can stop kudzu. With strong stomachs and voracious appetites, grazing goat herds keep kudzu at bay where labor-intensive chemical treatments and even prescribed burns fail.

Such is the state of Generative AI (GenAI) within the 2025 fraud landscape. Its invasive tendrils are spreading into almost every fraud vector at an overwhelming pace. It's likely the reason why, despite increased investment in fraud prevention, **41% of businesses continue to have a high level of concern about the risk of fraud.** It's also believed to be at the root of the **14% year-over-year growth in fraud loss.**[3,4]

But stopping GenAI-powered fraud doesn't require setting your strategy on fire. Despite the overwhelming creep of the GenAI weed, it's still just a weed. Invasive? Yes. Unstoppable? No. You've cut down weeds before. This one might be more aggressive and fast-growing, but it doesn't have to be invasive. Straightforward approaches (think: herds of goats) can help tremendously.

Southern gardeners know to focus on controlling the impact rather than trying to uproot the invasive spread. In 2025, successful fraud teams will take a similar root — er, route. **Let's talk about the kudzu, the invading GenAI menace and the goats of 2025's fraud ecosystem.**

Untangling the GenAI Vines Across Attack Points

Based on the industry surveys and research summarized in the *Experian 2024 Identity and Fraud Report*, NeuroID's fraud attack data database and our internal fraud expertise, we've compiled the trends we anticipate will impact fraud leaders the most in 2025 and how you can get ahead of them. Every trend has been heightened by the growth of GenAI, and our focus is on helping you manage each creeping threat — such as next-gen bot attacks, new account fraud and escalating fraud attack aggression — while working within the reality that there is no one single solution. But by focusing on specific vectors, you can control the impact even if you can't stop the invasive GenAI spread.

Top Most Encountered Fraud Events Reported in **2023**

- **#1** Account Takeover Fraud
- **#2** Identity Theft
- **#3** New Account Opening Fraud

Top Most Encountered Fraud Events Reported in **First Half of 2024**[5]

- **#1** Identity Theft
- **#2** APP Fraud
- **#3** New Account Opening Fraud

Trend 1: Identity Theft & New Account Fraud Will Continue to Rise

In the first months of 2024, identity (ID) theft officially claimed first place as the most experienced type of fraud reported by businesses. It was in second place in 2023: in 2024, it not only rose, but knocked 2023 reigning champ account takeover (ATO) fraud out of the top three entirely.[6]

ID theft is bread-and-butter fraud that you've been fighting for decades. So why is this basic fraud type topping the list of most encountered? Shouldn't we in the fraud world have solved this already?

The surge in ID theft is one of the fast-growing vines on the GenAI kudzu. We can assume it's because of the ease with which GenAI and next-generation bots are able to exploit stolen personally identifiable information (PII) at scale. Compromised PII has long-fueled ID theft, and now GenAI and other advanced technology makes it easier to find and misuse PII at scale. **GenAI can scour the internet for stolen data and build automated attacks far faster than any humans or previous generation bots.**[7]

Which brings us to another bud on that thorny vine of 2025 trends: new account opening fraud, the third-most experienced fraud event in the first half of 2024. ID theft and new account fraud sprout together on one fast-growing GenAI vine, as ID theft is easiest to perpetrate at new account opening.

Compromised PII is endlessly available on the Dark Web and the problem will only continue to grow: in 2024, more than 1B people in the U.S. were impacted by a data breach — a **409% increase over 2023.**[8] Fraudsters use this compromised data to probe websites and apps, testing for weak fraud controls. In some cases, fraudsters don't even need to open an actual account to commit new account fraud. NeuroID's data reveals instances where fraudsters go through the application process only to drop off after using pre-fill functions — **a tactic observed 6K times by one customer alone**. This is a tell-tale sign that an application is being used for PII harvesting: a fraud technique where an application inadvertently leaks valuable customer data (common in pre-fill set-ups). For example, an application confirming a vehicle or city of residence provides a fraudster with answers to common KBA questions. Even by confirming a username and password belong together, you can inadvertently leak consumer information.

With all that leaked PII, fraudsters can easily upgrade their bot attack styles, enabling ID theft and new account fraud to grow their roots even deeper.[9] Early bot detection methods like IP blocklisting, user-agent analysis and basic behavioral heuristics were effective against earlier generation fraud bots who showed predictable, inhuman patterns. But as detection methods advanced so did bots, using generative learning to specifically evade these tools.[10] Attackers have created bots that behave nearly identical to real human users and are able to overcome each barrier.

To test how deep next-gen bots were reaching, NeuroID data scientists evaluated attacks on 55 financial services providers over a seven-week period. They found that **71% of these companies experienced bot attacks in that timeframe.** And of those attacked, **43% were hit by next-generation fraud bots almost exclusively.** Next-generation fraud bots, also called fourth-gen bots, are more prevalent and sophisticated than expected. And they're likely helping supercharge ID theft and new account fraud.[11]

The Thorny Vine: Overengineered Fraud Stacks

In theory, your fraud stack should be a dynamic workflow. But as fraud evolved, a throw-the-kitchen-sink-at-it approach took hold. It's an understandable response: as fraud advances at a lightning pace, add solutions to fill the unseen gaps and trust that they'll be closed.

But this approach has created fraud stacks full of redundancies and fraud professionals who must spend exorbitant amounts of time digging through data to understand attacks. It's inefficient and often doesn't add insights into the efficacy of each fraud stack component, nor the attacks making it through. Plus fraud tools aren't cheap. The more tools you throw into your stack, the more you're eating into your margin (without a clear understanding of the ROI that each tool provides).

The Goat: Orchestrated Data Calls for Improved Attribution

A critical starting point for 2025 is knowing what tool is catching specific fraud. This basic insight enables you to better identify and track your entire fraud stack's performance and provides deeper looks into fraud attack vectors and vulnerabilities.

One of the most effective ways to improve visibility into stack performance is through orchestrated data calls rather than simultaneous, all-at-once processing. With orchestrated calls, you can intelligently determine - based on KRIs, available data and outcomes from prior calls - which fraud tool(s) should be called next and whether they should be called sequentially or in parallel. This enables you to attribute specific risk detection to the appropriate tool, making it easier to understand which signals are flagging potential threats and which might be falling short.

In a well-orchestrated fraud stack, early tools placed higher up in the fraud stack provide no friction, have exceptional third-party fraud capture (and especially bot capture), lower false positives and are cost-optimized. These early filters stop fraud before you need to spend money on more costly identity, compliance and credit processes. For example, a behavioral analytics solution might flag high-risk applicants before they even hit submit, letting you toss them out immediately. Then, second tier tools in the fraud funnel can be applied to users that make it past the first-tier tools. These catch more focused and complex fraud vectors, such first-party fraud. While those types of solutions and models can be more expensive, they don't need to be applied to your entire population of users if you filter out the top-of-funnel fraudsters.

Cutting through the infestation of GenAI-powered ID theft and new account fraud can start as simple as this: **Use knockout criteria, adjust waterfall rules, implement hard declines and do an overall workflow evaluation to ensure initial checks catch the highest-risk applicants, with progressively more detailed checks following.** If you can't make these adjustments, then the hard truth is you won't be able to tell how performant your tools are. **You'll continue to miss the gaps where GenAI roots dig in and lodge deep.** If your infrastructure is too linear and rigid for these adjustments, then that is a clear sign that coming into 2025 you need to invest in more modern technology that can adapt not just for sequential testing, but for staying ahead of new fraud types.

Without untangling the data, you'll miss the insights. And these fraud attacks are only expected to grow in size, scale and sophistication. If you can't find the holes in your stack, how will you be able to repair them?

Trend 2: APP Scams Will Continue to Grow

On the opposite end from tried-and-true ID theft are the relatively new vectors of real-time payments (RTP) fraud. With 2024's rapid adoption of FedNow, RTPs have created a new world of instant fraud. **Authorized Push Payment (APP) fraud, perhaps the most insidious form of RTP fraud, came in second for the most experienced fraud attempt in the first half of 2024.** Twelve percent of respondents also said their most important investment area for 2024 was "improving how we detect and prevent APP fraud."[12]

APP fraud preys on trust, as cybercriminals convince victims to make urgent fund transfers. Then near-instant payment settlement makes their losses irrevocable. APP fraud and other real-time fraud types are already overwhelming RTP systems in the UK, where **40% of fraud incidents are attributed to real-time payments.**[13]

In 2025 and beyond, we expect the U.S. to face similar fraud spikes as RTP usage expands, especially in peer-to-peer (P2P) and business payments.[14] With 85% of U.S. consumers asking for real-time payments from businesses[15] and FedNow continuing to roll-out, real-time is unlikely to slow down.[16] Already in 2023, an average of **$100 million was sent over the Zelle network every hour,** at a growth rate of 28% year-over-year.[17]

The Thorny Vine: Evolving Regulations and Threats

RTP adoption is in early stages in the U.S., but any combination of increased volumes and speed pose serious fraud challenges for large payment processors and banks. **The challenge extends beyond detection and prevention, as regulators and financial institutions (FIs) alike grapple with understanding where responsibility lies in detecting and stopping these scams.**

Unlike other fraud types where no one can fully tell how GenAI is specifically being used to commit fraud (unfortunately, fraudsters didn't return our calls for quotes), the influence of GenAI on APP fraud is glaringly clear: cybercriminals use GenAI tools to create deepfake content that makes their scams believable. But determining responsibility is complex, especially in the U.S., where regulations on RTPs are still evolving and the burden of responsibility is being debated.

Looking to the UK, we can see the complexity of GenAI kudzu and how it might reach its vines into our own RTP landscape. In 2022, the UK's Payment Systems Regulator (PSR) proposed holding banks and fintech companies liable for up to £415K when customers fall victim to APP and similar payment scams. The financial industry shifted blame to social platforms (such as Meta and WhatsApp) where many scams originate. As of 2023, the law states that banks and fintech firms are responsible for reimbursing customers up to £85K, with liability split equally between sending and receiving banks. But there's yet to be a formal mechanism enacted for coordinating reimbursements between banks, leading to a huge reliance on manual processes.[18] **Individual banks are left to figure out the balance of ensuring consumers are informed, without overwhelming their fraud teams** (one novel approach: UK banking app Revolut requires customers to take a selfie holding a sign that reads "Revolut warned me this is likely a scam and I am unlikely to get my money back," then send it to the app before they can proceed to authorize certain suspicious transactions[19]).

Whether or not clear regulations are in place, FIs face significant consequences from APP fraud. If protection measures are inadequate, you must deal with the reputational fallout of victims, but the operational burden. Either approach requires a bolstering of internal controls and fraud prevention strategies to minimize risk and protect both victims and your business reputations.

The Goat: Post-Onboarding Fraud Mitigation

Fraud mitigation that stops at the onboarding phase is missing scams. Post-onboarding fraud detection is essential to safeguarding accounts and reducing exposure to APP fraud and other real-time scams. This includes implementing stronger login protections and ensuring that only verified, trusted users can access accounts.

Older device and network solutions, which often rely on limited-timeframe device recognition, are inadequate against GenAI-enhanced tactics. These outdated methods lack the capability to maintain persistent device IDs, leaving them vulnerable to spoofing attempts and other adaptive strategies employed by real-time focused fraudsters. **Behavioral analytics, device fingerprinting and GenAI-driven anomaly detection are straightforward, goat-level approaches for identifying suspicious behavior beyond login.** While regulations and responsibilities continue to evolve, these measures help create a safer environment for users and reduce the likelihood of APP fraud succeeding.

The good news is that fraudsters equipped with GenAI use sophisticated probing techniques, adjusting variables such as VPNs and IP addresses to identify security gaps. Persistent device ID technology enables tracking of these interaction patterns, creating a robust defense against these tell-tale tactics.

As GenAI remains endlessly adaptive, so must your solutions. Perhaps this comes in the form of progressive friction application that corresponds to the risk attempted. Consumers say they expect, and even want, a certain level of friction from their FIs: 48% "are more trusting of businesses when they demonstrate signs of security."[20] This is where your fraud stack needs flexibility in detection that introduces a range of nuanced variables for fraudsters to decipher. This added complexity makes it difficult for attackers to determine which specific actions trigger security alerts, effectively slowing down their ability to adapt — and speeding up yours.

Scams are thorny and are only going to get more complex. But multi-pronged, behind-the-scenes infrastructure enhancements can prevent your customers' exposure to cybercriminals and lessen the likelihood they'll fall for these malicious manipulations.

Trend 3: More Aggressive Fraud Attacks from Every Source

NeuroID data scientists have tracked the the latest shifts in not just fraud methodologies, but overall fraud aggression. For example, compared to January 2023, **January 2024 had a 50% reduction in the number of fraud attack attempts**, and this trend continued into February and March, with a 54% reduction in February 2024 attacks compared to 2023, and a 64% reduction in March attacks compared to 2023.

The Thorny Vine: Brute Force, Sustained Attacks

But it's not all good news. Despite the fewer attacks, the average number of risky users associated with each attack in January 2024 **increased by 47%** over January 2023: essentially doubling the impact of each individual attack. February was even more striking, with a **95% increase** in attackers per attack. And in July 2024 fraudsters rallied their troops (most likely bots) for a **3X increase in the number of risky users** per attack compared to the same timeframe in 2023.

So, while attacks are fewer, they are far more aggressive with a higher number of risky users showing up for extended bombardments. Fraudsters aren't giving up after one attempt and moving on but are doubling down on their victims — an evolution in aggression that suggests an adoption of tools that enable highly focused and effective attacks.[21]

The Goat: Cross-Industry Collaboration

The siloed nature of the FI industry can be a huge advantage for fraudsters. Of course, FIs aren't eager to tell the public or their competitors that they're being attacked by cybercriminals. **This secrecy gives said criminals the freedom to learn from attacking your competitor, then refine their approach when they come after you.**

A recent U.S. Treasury report ranked information sharing as one of the most crucial components to an effective fraud defense, suggesting that **"financial institutions should . . . enhance collaboration, particularly threat information sharing"** just as much as they should strengthen their risk management.[22] This lack of fraud-related data sharing is especially harmful to smaller or newer FIs, who don't have a wide base of historical fraud data to examine for pattern detection. At the same time, they are also often the first to experience attacks, as fraudsters assume their defenses will be less sophisticated. In this way, smaller FIs can serve as canaries in the coal mine for bigger banks as to what's on the horizon of fraud rings and bot attacks.

We're not saying you should email all your fraud attack data to your closest competitor. But there are other effective ways to both support and learn from your peers.

Fraud solution vendors, with their broad client base and long-tail industry insights, are a great resource to help you understand and prepare for upcoming attacks. A collaborative vendor relationship based on outcome data transparency can lead to powerful, reciprocal knowledge-sharing to support your fraud goals. Many vendors even have advisory boards, where industry insights and trends are regularly shared. These boards offer a unique opportunity to get informed on the types of attacks hitting the entire market, so you can better understand if your experiences are isolated incidents or growing trends (and adapt your response accordingly). **Of course, these vendors are also selling products: but a relationship should be part of that product package (and if it's a solution you need anyway, maybe that trust is a differentiator to help you choose between vendors)**.

Surveys and conferences hosted by industry leaders and government regulators also help provide more panoramic views of fraud tactics, attack vectors and successful defense mechanisms. Building alliances with peers and vendors alike across the industry ensures you're part of an informed and agile goat herd, ready to feast on the fast-growing kudzu of fraud.

The Goat Approach To 2025 Fraud

GenAI is invasive and intimidating — you can't bushwack the entire weed and the roots have already taken hold. It lowers the barrier of entry for fraudsters to employ more dynamic attacks, from creating advanced bots to rapid IP hopping and faking documents. It has redefined the fraud landscape for good and is expected to be the cause of **quadrupled fraud losses by 2027, with a staggering annual growth rate of more than 30%.**[23]

Unfortunately, fraudsters aren't filling out surveys about their new methodologies and techniques. We can only make assumptions about how they're using GenAI and other next-gen technology based on attack trends.

But at the end of the day, does it matter? You don't need to know the plant that's strangling your garden is called kudzu — you just need to know how to stop it from climbing through the windows of your house.

And you don't have to *stop* GenAI, you just need the right goats to set loose in the right fields. Coming into 2025, focus on staying strategic, closing the vectors you can, remaining flexible and unleashing some hungry goats to do what they do best.

Want to learn more about behavioral analytics and if it could be the right goat for your 2025 fraud stack?

Read *The 2025 Buyer's Guide to Behavioral Analytics for Fraud Prevention* for use cases, strategic considerations, integration details and more.

NeuroID, a part of Experian, offers a friction-free, privacy-centered, and tailored solution to digital identity screening. After more than a decade of researching human-online interactions, our solutions provide a front line of defense by differentiating between genuine users and potential threats in real-time. NeuroID solutions assess a user's intent — be it a genuine prospect, fraudster, or bot — by analyzing their interactions with a digital device. Our unique crowd-level insights, paired with expert guidance support modern risk management so global leaders can see fraud faster, reduce losses, and increase savings.

1. Kudzu: The Invasive Vine that Ate the South, Nature.org, accessed Nov. 2024
2. How Kudzu Works, HowStuffWorks, accessed Nov. 2024
3. Federal Trade Commission, Explore Data, Nov. 2024
4. Regulatory Alert - Fraud, Identity Theft and Other Scams, KPMG, accessed Nov. 2024
5. Experian's 2024 Identity and Fraud Report Highlights Evolving Fraud Landscape
6. Experian's 2024 Identity and Fraud Report Highlights Evolving Fraud Landscape 7.
7. New Industry Report: Are Fraud Bots Beating Behavioral Analytics?, NeuroID 2024
8. 2024 Threat Detection Report, Red Canary, accessed 2024
9. New Industry Report: Are Fraud Bots Beating Behavioral Analytics?, NeuroID 2024
10. Next Generation Bots Pose Formidable Fraud Challenge, Payments Journal, accessed Nov. 2024
11. New Industry Report: Are Fraud Bots Beating Behavioral Analytics?, NeuroID 2024
12. Experian's 2024 Identity and Fraud Report Highlights Evolving Fraud Landscape
13. Is the UK Brexiting From Instant Payments?, PYMNTS, accessed Nov. 2024
14. Real-Time Payments Fraud Is Growing - Here's How to Prevent It, T.J. Horan, FICO, 2023, accessed Nov. 2024
15. 3 Common Myths About Real-Time Money Movement & Fraud, NeuroID 2023
16. 5 Payment Trends in Fintech: Emerging Payment Technologies, Discover, 2022, accessed Nov. 2024
17. Zelle soars with $806 billion transaction volume, up 28% from prior year, PRNewsWire, 2024, accessed Nov. 2024
18. Faster Payments APP scams reimbursement requirement, PSR report, 2024, accessed Nov. 2024
19. Why Revolut is asking suspected scam victims to take selfies, Telegraph, 2024, accessed Nov. 2024
20. Experian's 2024 Identity and Fraud Report Highlights Evolving Fraud Landscape
21. Q1 Emerging Attack Trends
22. Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector, U.S. Department of the Treasury, 2024, accessed Nov. 2024
23. Generative AI Is Expected To Magnify The Risk of Deep Fakes and Other Fraud In Banking, Deloitte Report, 2024, accessed Nov. 2024