neuroID

WHITE PAPER • JANUARY 2024

The 2024 Fraud Stack Audit: A Guide to Balancing Fraud, Friction, & Finance

Today's fraud stacks are full of inefficiencies that slow down conversions. They create the equivalent of hours of security footage to review by collecting so many signals that it's impossible to untangle and prioritize.

Entering this new year of economic uncertainty and fast-paced fraud, fraud teams are being asked to re-evaluate the effectiveness of their stack. Here's where to start.

McKinsey & Company

A New Approach to Fighting Fraud while Enhancing Customer Experience, 2022

> The evolution of fraud threats has undermined the effectiveness of a reactive approach to combating fraud, which essentially focuses on stopping schemes one by one through manual reviews.

2023's shadows of economic uncertainty are expected to stretch into 2024. These shadows will undoubtedly reach into the corners of fraud prevention: when the economy trends downward, fraud goes up. We saw it in 2008 when personal identity fraud rose to peak levels on the heels of the global economic crisis[1] and we saw it again in 2020, when the FTC received 2.2 million fraud reports in the midst of COVID-driven economic uncertainty.[2] Today, we're facing similar rising unemployment, fluctuating interest rates, and banking turmoil.[3] Coming into 2024, this global financial instability is likely to inspire both casual fraudsters and large-scale fraud rings to supplement their incomes.

At the same time, fraud prevention professionals are feeling the pressure to cut costs. A recent Deloitte report found that more than half of CFOs are going into cost management mode.[4] The fintech sector is especially feeling this crunch, as the previous growth-at-all-cost mindset transitions to a do-more-with-less mentality. There's an industry-wide push to focus on efficiency and reassess operating models for scalability and simplification. In this economic climate, every investment in fraud prevention is closely scrutinized for its direct and indirect impact on profit margins.[5]

In the midst of this cost-conscious environment, fraud techniques have evolved at an unprecedented pace. Advancements in generative AI,[6] sophisticated bots,[7] deepfake capabilities, and vulnerabilities within new instant payment systems have streamlined the process for bad actors, challenging traditional fraud prevention stacks that primarily rely on personal identifying information (PII) verification. Fraud professionals are facing new challenges with old tools, and now they have moths flying out of their empty wallets, making it harder to upgrade.

1. Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back
2. New Data shows FTC Received 22 Million Fraud Reports
3. 3 Strategies for Navigating the New Banking Landscape | NeuroID
4. CFOs Share Perspectives, Priorities, and Plans for 2023 - WSJ
5. Webinar: Fight Fraud, Not Finance | NeuroID
6. How GenAI Supercharges Fraud—and How to Fight Back | NeuroID
7. Emerging Trends in Bot Attacks | NeuroID

As financial institutions (FIs) enter 2024, the need for cost-optimized, adaptive, and advanced fraud prevention is clear. So, where do you start?

Over-Layered and Under-Performing: Re-Evaluating Today's Fraud Stack

Balancing fraud, friction, and financial impact is a complex problem and it has created a complex fraud stack. In an ideal world, a fraud stack contains layers of security measures that create a comprehensive defense. But in reality, today's fraud stacks are full of inefficiencies that slow down conversions. They create the equivalent of hours of security footage to review by collecting so many signals that it's too much information to efficiently prioritize.

Because even as you add layers, fraudsters continue to evolve. They have personal data at their fingertips and advanced technology that was built specifically to fool many of today's identity verification and validation systems. Digital bad actors, such as members of fraud rings, commonly use compromised personal identifying information (PII) to commit new account opening fraud and take advantage of inadequately defended companies.[8]

Insurers, fintechs, and every other business where money moves online, are all at risk if they depend solely on any of the multiple forms of PII-data capturing systems for identity verification and fraud detection.[5] The bad actors know this, which is why they're constantly searching for access to PII. Whether it comes from data breaches, phishing schemes, the dark web, or other sources, they'll take any information they can get.[6] That's why no matter how high your fraud layers are stacked, if they're built on PII data, they're on a shaky foundation.

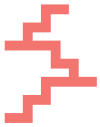
Deloitte
CFO Journal, 2023

> . . . With the continued uncertainty, cost management is going to be critical . . . . For example, CFOs are spending more and more time with their supply chain leaders to understand the drivers of costs and explore ways to stabilize them.

8. The PII Well is Poisoned. Here's What You Can Do About It | NeuroID

Red Flags of an Outdated Fraud Stack

Manual Step-Ups



Many digital businesses still use manual processes to verify customer identities. This approach is notoriously expensive, difficult to scale, and error-prone. It introduces high levels of friction and applicants have to wait hours or days for approval, which leads to drop-off and abandonment.

Friction Filled Approaches

For example, an onboarding process that requires hours or days for prospects to be approved. Identity documentation matching, for example, often requires prospects to go through the arduous process of taking a photo that requires complicated movements and tests to prove "liveness," and then be put into limbo and escalated to a lengthy internal review . . . in the meantime, they take their business elsewhere or simply lose interest.

Considering Fraud as a Business Cost

47% of companies experienced a fraud incident between 2020 and 2021, and fraud is estimated to have cost online businesses more than $20 billion in 2021 alone. It is estimated that there are more than 41 different types of fraud attack strategies (and those are just the schemes we know about). While not all businesses are vulnerable to every type of fraud, both of those figures—the costs and the number of schemes—are only expected to grow as fraudsters become more creative and sophisticated with the adoption of new technology and channels. Some businesses choose to think of fraud loss as just a cost of doing business. But high fraud losses are a broader warning sign that you're ignoring crucial identity verification gaps.

There are also more 'citizen fraudsters' taking advantage of lower barriers of entry and fast cash grabs. In Aite-Novarica's 2022 report on emerging fraud trends, they predicted that "fraudsters of all stripes" would migrate to "forms of fraud that require relatively little in the way of technical proficiency and that are dependent on the use of stolen and synthetic identities."[9]

We're now seeing this play out in everything from 'scam bibles' sold on TikTok to genAI-based phishing attempts. There are endless opportunities to compel everyday people to simply dip a toe into the fraud pool now and then.[10] And when we look at the evolution of fraudsters, we don't mean just the technology sophistication, but also a wave of new strategies. Fraudsters can be patient and methodical, as they've learned to test systems by deliberately going through step-ups and denials, or even purposefully building up credit for a year or more before striking.[9]

FiVerity

2021 Synthetic Identity Fraud Report

Fraudsters can take as long as 18 months to build up their credit and then strike—the average synthetic identity fraudster profile successfully steals between $81,000 and $98,000.

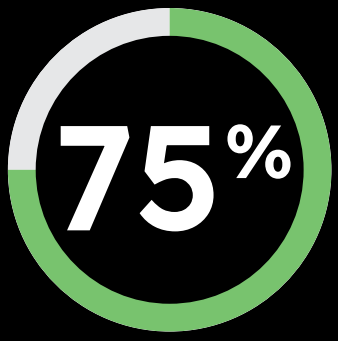
9. Stark Reality of Identity Theft | Aite
10. 2021 Identity Fraud Study: Shifting Angles | Javelin

Recognizing the Hard Impact of "Soft Costs"

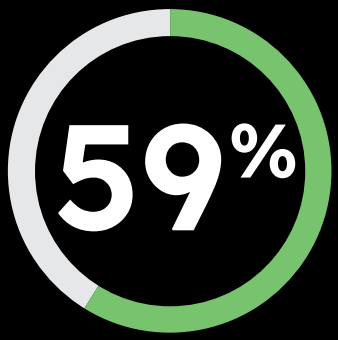
Even as fraud methodologies become more sophisticated, tech stacks have stagnated. During the fintech years of economic expansion, it was fine to throw money at the problem through ad hoc point solutions: add digital ID verification to your PII checks, for example, or more complex step-ups. But with today's tightened spending, optimization, not addition, is the goal. Siloed solutions have limited scalability and flexibility to keep up with the evolving nature of digital fraud. With the pressure to deliver financial results increasing, fraud stacks are facing greater cost scrutiny.

Fraud professionals are seeing more of the impact on the bottom-line of fraud prevention inefficiencies, as well.[11] These come in the form of ancillary expenses and multifaceted "soft costs." Soft costs can include the extra dollars spent on step-up API calls for each layer in the fraud stack and the human hours dedicated to manual reviews. Then when those tools don't work, the soft costs transfer to the expense of repairing reputational damage from breaches. These can also be profound and far-reaching: digital fraud victims are 3x more likely[10] to leave the FI that they hold responsible.

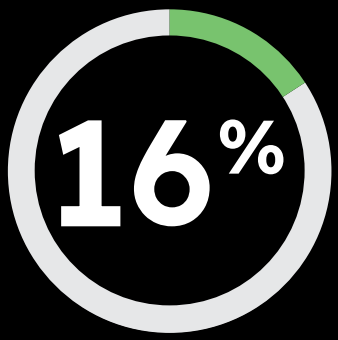
Overengineering without solving the problem is now becoming the problem, as a holistic view of your fraud landscape gets hidden under layers of disjointed point solutions and cascading costs. Throwing more money and vendor layers at the digital identity fraud problem is no longer the solution. Instead, it's time to closely examine the multi-layered, heavily enriched fraud stack configurations and streamline for top-of-funnel efficiencies that can actually help customer conversions.



of digital businesses said their manual review costs increased in 2022



of digital businesses expected to lose more revenue to fraud YoY



increase in true fraud incident cost since 2020; now, every $1 of fraud is estimated to actually cost a company close to $5.

Survey Finds Fraud Costs Rising for Banks | Banking Journal
State of Online Fraud | Stripe
Top Fraud Trends 2023 | Data Advisor

11. What Are NeuroID Customers Most Worried About When Facing the 2024 Fraud Landscape? | NeuroID

Use Case

How a Sophisticated Fraud Ring Snuck Through an Overly Complex Fraud Stack

The Attack
A fraud ring was targeting the pre-qualification process of a major credit card issuer. The attackers initially conducted a probing test to understand the issuer's control mechanisms. They then adapted their tactics to evade detection, essentially using the issuer's existing digital identity and verification systems against them.

The Defense
NeuroID's behavioral analytics stepped in as a critical line of defense. Unlike conventional methods such as PII tracing, credit reports, and device fingerprinting, which the fraud ring skillfully circumvented, NeuroID's behavioral analytics flagged the attack in real-time.

The Outcome
NeuroID successfully identified these attacks as coordinated and large-scale. Remarkably, one-third of the fraud ring users were flagged exclusively by NeuroID. These individuals would have otherwise slipped through the issuer's verification layers undetected.

READ THE FULL STORY

Saving Money and Streamlining Onboarding: Simplifying the Stack

According to research firm Aite-Novarica, business losses from identity theft will grow to $635.4 billion by the end of 2023.[9] Facing a gathering storm of increasing fraud, decreasing spend, and overengineered fraud stacks, now is the time to find ways to work smarter within holistic approaches in order to secure growth. It's time to streamline processes and pay attention to what a fraud stack is influencing beyond its prevention goals: such as false positives and unnecessary friction, both of which can cause slow approvals and hurt conversions. The more steps in an onboarding process, the more likely customers are to drop-off (translation: the more layers, the more drop-offs).[12]

Behavioral analytics are where many digital businesses are looking first, for its benefits in reducing fraud risk and false positives, without adding to the fraud stack. Best-in-class behavioral analytics add no friction to the onboarding process, are undetectable to your customers, and live on that pre-submit level—using data that is already captured by your existing application process. Without requiring any new inputs from your potential customers or stepping into messy biometric legal gray areas,[13] behavioral analytics use AI-driven analysis to aggregate, sort and review a broad range of cross-channel, historical and current customer behaviors to develop clear, real-time portraits of transactional risks.

12. The Privacy Calculus and the Power of Progressive Onboarding | NeuroID
13. Biometrics and Behavioral Analytics Explained | NeuroID

Stolen PII or real log-in credentials don't impact the results, because behavioral analytics look at abnormal aspects of the bad actors' activity. Behavioral analytics rely on a customer's pre-submit digital body language of taps, keystrokes, swipes, backspaces, pastes, tabs, clicks, etc. as users complete online forms—to reveal authenticity (or inauthenticity), malicious intent, fraudulent behavior (whether from a singular actor, a bot, or a fraud ring), and more with startling accuracy. This gives behavioral analytics astonishing predictive power, while securing both fraud prevention and ease of customer onboarding. It's a passive layer within your stack, adding zero friction to the end-customer.

Start at the Very Beginning: Untangling Bottom-Line Costs from the Top-Down

A good first step to detangling the overly engineered and ensuring effective fraud prevention is to focus on the start of your applicant journey at the top-most peak of the onboarding funnel: the pre-submit phase, before an applicant even clicks the "submit" button to enter their data.

By interpreting these behavioral signals at pre-submit, users are tagged with a friction-right conversion approach:

• **Low Friction:** Applicants familiar with the data they've input are likely who they claim to be. Friction can be optimized to move them through the process faster, for fewer false positives and less UX-based conversion loss.

• **High Friction:** Applicants showing low-familiarity with the data they've input are tagged as risky. Friction can be optimized to include additional step-up authentication for these threats, so they are weeded out instead of being allowed to spread seeds of fraud throughout a business ecosystem, and making efficient use of a fraud stack instead of applying an expensive blanket treatment.

Fraud prevention and detection is still a vital part of this onboarding—but now it is tailored to the preferred user's experience, as determined by the initial capture of friction-free behavioral signals. This untangles the fraud stack significantly: no more forcing multi-layered checks and step-ups that can turn into tedious onboardings that often hurt genuine customers more than fraudsters (in one particularly rough example we saw, a customer found that prior to NeuroID, their friction balance made it actually easier for bots to get through onboarding and harder for their than genuine users).[14]

Create a More Streamlined Stack with Behavioral Analytics

Facing 2024's fraud landscape, modern and efficient solutions are key to success. Behavioral analytics look for intent signals before a user even hits "submit," and then appropriately flags that intent as genuine (and able to be fast-tracked through needless friction) or risky. If flagged as risky, that's when the post-submit, traditional fraud stack will come into play for step-ups and escalated checks. Detangled at the start of the customer journey, each prospect can follow a straight line either into your ecosystem or away from it, depending on their behavior, without triggering complex, costly stacks of signal checks.

Behavioral analytics helps you make the most of your fraud stack by giving it the right information to do its job, instead of forcing customers to travel a winding road of overengineered point solutions.

Talk to an expert today for a tailored demonstration of what behavioral analytics could do for your fraud stack.

14. Insights from the Frontline of Fraud | NeuroID

NeuroID, the global leader in behavioral analytics, offers a friction-free and privacy-centered 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.