neuroID

WHITE PAPER • NOVEMBER 2023

Anatomy of a Fraud Ring Attack

Breaking Down 5 Digital Fraud Ring Attacks: The Victims, The Ringleaders, and The Results

The Association of Certified Fraud Examiners estimates that **annual global fraud losses total nearly $5 trillion.** A large fraud ring working in an organized attack can do more financial damage than any individual fraudster ever will. **The more individuals, the more complex the attack.**[1]

The phrase “fraud ring attack” strikes fear in the hearts of every fraud, risk, and compliance team. If you’re lucky, you’ve only read the endless headlines about the devastating impacts of fraud rings, which cause an estimated **$5 trillion in financial damages every year.** If you’re unlucky, you’re one of the thousands of companies who have experienced the overwhelming frenzy of a fraud ring attack first-hand.

At the height of the pandemic, headline after headline told stories of online fraud perpetrated by ‘citizen fraudster’ opportunists taking advantage of the unprecedented push to digitization. These citizen fraudsters are to fraud rings what a dine-and-dash college student is to a mafia hitman. They saw a gap and took advantage, but they don’t make their living as professional, organized cybercriminals. But at the same time, there was an equivalent surge in fraud rings. **As the increasingly aggressive fraud landscape caused prevention tactics to grow more sophisticated, fraud rings evolved in kind.** Ringleaders became more organized and aggressive: since 2020, fraud ring attacks have nearly doubled.[2]

Fraud rings are extremely cunning, patient, and focused, even taking the time to learn about their targets step-up policies and identity verification procedures. **They typically test out different fraud schemes to discover how their targets react before they make the real attack.**[3] They’re looking to gather as much information as they can in order to land on the best angle of assault—and their research would put even the most diligent PhD student to shame.

[1] Protection Against Organized Fraud, fraud.net/d/fraud-ring/

[2] PwC’s Global Economic Crime and Fraud Survey 2022, www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

[3] The Crowd Goes Wild, Edition 2, https://neuro-id.com/resource/report/emerging-trends-in-bot-attacks-insights-from-the-frontline-of-fraud/

For Every Ring There is a Season

Fraud rings know to take advantage of timing as well. For example, they might strategically attack during Christmas—or even Valentine’s Day, back-to-school season, Mother’s Day, etc.—blending in with your rush of good customers. They know you’ll be especially averse to adding step-ups or similar friction during a high traffic period and more focused on preventing delays and false positives for good customers, rather than looking for fraudsters.

Similarly, fraud rings follow the money: if you’re a fintech that publicizes growth or financing, they’ll know that you have new funds to exploit and that you likely don’t have a robust fraud prevention strategy yet, since you’re focused on hyper-growth. **We’ve seen fraudsters get so precise as to explore the possibilities of attacking at different times of the day.**

This hyper-detail and patient attack strategy is part of why fraud rings are so difficult to detect. You might have a reassuringly consistent level of fraud attempts, then out of nowhere get hit by a brutal ring that blitzes in to overwhelm your system. And it’s never a one-and-done: fraud rings rinse-and-repeat. As soon as they find a weakness, they’ll double down and squeeze it as much as they can.

The Anatomy of a Fraud Ring Attack

While the style of the fraud ring varies based on the target, the tell-tale signs are there for those who know how to interpret them. For example, high velocity is often thought of as a fraud ring indicator. And that’s true—if a single user tries to make several purchases in a short period of time, they could be a fraud ring member capitalizing on a successful point of attack. Or they could be a grandma, remembering that she needs to buy the same toy for her grandkids so they don’t argue over it (or any other number of innocuous reasons). In the end, there’s very little you can tell from just one data point.

Fraud rings are fast, frequent, and furtive. It takes a multi-layered approach to pull them from the shadows, but it’s well worth it. Uncovering their tracks is invaluable for preventing revenue loss from fraud, false positives, and friction. It’s the only way to prevent future attacks—including those by accounts that are part of the ring and made it into your system as “sleeper fraud.” It’s only after you’ve identified a fraud ring that you can see the transactions that match its behavior and act accordingly to save yourself from attacks in-progress or incoming soon.

A Little Knowledge is a Dangerous Ring

Some Ways that Fraud Rings Test Boundaries Before an Attack:

- Targeting a merchant to see what channels and purchase instruments they accept, which they step up, and which they reject.
- Social engineering research to discover how data is stored and how long before chargebacks occur.
- Looking for a variety of vulnerabilities in the site, such as dollar thresholds for when fraud screening steps up, when they’re sent to manual reviews, and what machine learning rules are applied.
- Attempting basic hacking and analyzing how the site responds.
- Examining how time and seasons impact change—are there more lenient fraud policies during peak holiday season, for example.

NeuroID Sees Fraud Ring Attacks Every Day, Across Every Industry

Our behavioral analytics tools look past simple flags and into the intent of every user. Here's a breakdown of five recent fraud ring attacks we've detected: why they happened, what we saw, and how the victims fought back.*

*These fraud ring attacks are presented in broad strokes to protect the anonymity of the victims.

1. Fraud Ring Attack Target: Digital Lender

High growth means high visibility, which leads to high risk. And few industries are more fast-growing than fintechs.[4] Major growth milestones are often a signal to fraud rings that there's a target with new money to be stolen—and these organized rings know just how and when to attack swiftly and efficiently.[5]

The Attack

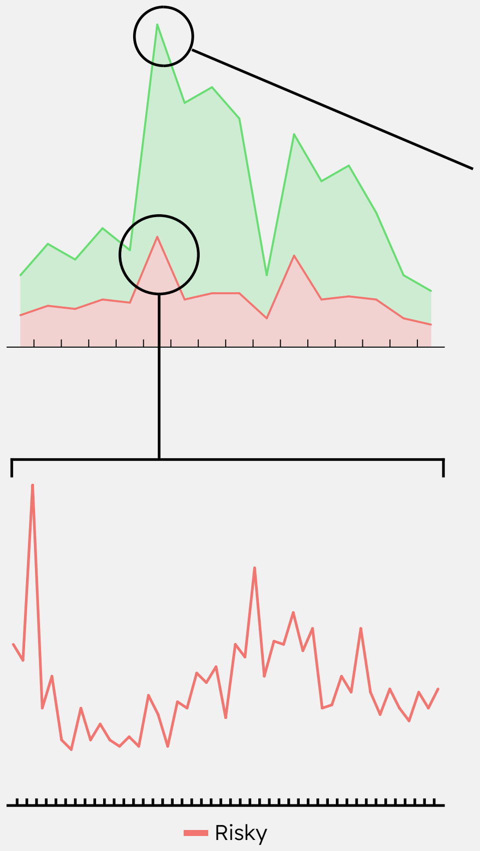
A credit card issuing hyper-growth fintech was celebrating: they had hit a new customer growth rate milestone and secured a new round of financing.

A sophisticated fraud ring caught wind of the issuer's success and attacked, with the goal of using a coordinated effort to overwhelm the system.

The Indicators

Abnormal, consistent spikes all from one particular acquisition channel were tell-tale signs of fraud ring activity. The issuer's fraud team started pending—and then outright declining—all applicants, even those above their typical risk ratio. False declines were potentially costing the issuer hundreds of thousands of dollars. But they couldn't afford to trust anyone while knowing such a highly aggressive attack was in progress.

NeuroID Fraud Ring Dashboard View



High-Velocity Spike in Genuine Applicants

A successful marketing campaign promoting their recent high growth led to a swell in genuine applicants (the green spike).

Not All Good News

The campaign announcing the fintech's high growth rate attracted a fraud ring (red spike). They likely counted on a large volume of applicants and loosely established fraud prevention.

[4] 3 Trends Driving the Growth of Modern Card Issuing Platforms in 2023, https://www.juniperresearch.com/blog/may-2023/trends-modern-card-issuing-platforms-2023-blog

[5] Inside the Next-Level Fraud Ring Scamming Billions Off Holiday Retailers https://www.darkreading.com/cyberattacks-data-breaches/inside-next-level-fraud-ring-scamming-billions-holiday-retailers

The Result

This attack spurred the lender to look for a fraud ring specific solution. NeuroID retroactively visualized their attack, helping identify similar patterns to prevent them in the future. Using NeuroID saved the issuer more than $800k in one four-week period by catching fraud rings and eliminating manual reviews of that data. **In a similar attack a year later, the lender used NeuroID to detect five risky fraud ring attacks in just six weeks.** One-third of the attackers bypassed other fraud tools in the stack and were only caught by behavioral analytics.

The Takeaway

Before NeuroID, this lender would have declined every applicant as soon as they recognized the fraud ring—eating the cost of false declines. This pull-up-the-drawbridge approach is a common panic-driven first reaction. But as fraud rings continue to evolve, the industry is realizing that the cost of false declines is sometimes even more impactful than the attack itself. Any future-forward fraud prevention stack will need to adjust accordingly. to better overcome the dual challenges of detecting fraud rings while protecting conversion rates.

NeuroID prevented $800K in fraud loss

1/3 of fraud ring applicants were **only tagged by NeuroID**

Earlier fraud ring detection led to operational savings

2. Fraud Ring Attack Target: Credit Union

We continue to see customers across industries sustaining a high level of fraud attacks—around one full-day attack every other week.[6] It's the nature of the business: as success increases, so does the target on the company's back. But as one expanding credit union saw, fraud rings have a unique brute-force attack style that can overwhelm defenses and derail growth.

The Attack

Months after expanding nationwide, a credit union looked to continue its growth by offering a promotion to new customers.

But when details on abusing the promotion were shared on the dark web, fraud rings wasted no time.

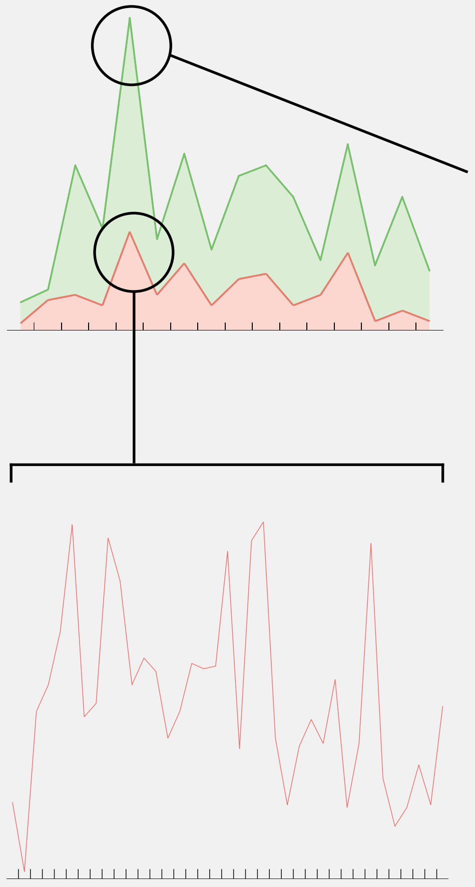
The Indicators

A 40% increase in risky behavior signaled that a fraud ring attack was underway. 70% of those risky users were completing the application, showing that these fraudsters were determined to infiltrate and wreak havoc. During large, coordinated attacks like this in the past, the credit union was forced to shut down its online application to manually review every application.

The Result

Prior to this fraud ring attack attempt, NeuroID had helped the credit union overhaul its fraud approach, **decreasing its daily applicant fraud volume by 35% and alleviating pressure on their manual review team.** NeuroID was able to trace this attack back to the credit union's marketing promotion, identifying the exploit that was attracting fraud rings and helping to prevent similar attacks in the future.

NeuroID Fraud Ring Dashboard View



High-Velocity Spike

A successful marketing campaign, promotion, or other traffic-creating event might cause a high-velocity applicant spike.

This is good news when the traffic is trustworthy.

Speedy Influx of Risk

In this case, there was also a speedy influx of risky traffic. These new applicants' behavior indicates they're unfamiliar with the PII they're entering.

This is bad news: the credit union was under long-term attack, with risky applicants hiding in the influx of trustworthy applicants.

[6] The Crowd Goes Wild, Edition 1, https://www.neuro-id.com/resource/report/use-case-snapshot-data-from-150-fraud-attack-attempts/

The Takeaway

The volume of coordinated fraud ring attacks can present an exhausting challenge for review teams and grind business to a halt. Stopping fraud faster and proactively protecting against attacks is crucial to taking pressure off fraud teams, reducing operational costs, and securing sustainable growth.

35% reduction in daily fraud applicant volume with NeuroID

1.4% lift on fraud detection rate

New insight into applicant segmentation and fraud patterns

3. Fraud Ring Attack Target: Merchant Onboarding

Enterprises that onboard customers—in this case, merchants—expect high levels of fraud attempts. Some merchant onboarding companies we work with have experienced upwards of $2 million stolen in a single fraud ring attempt and expect up to 15% of users to be fraudulent actors, just as a baseline.

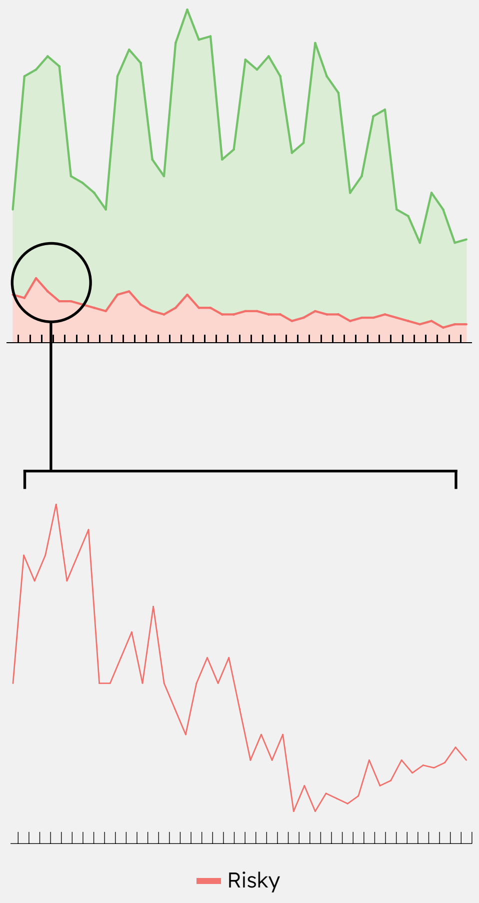
The Attack

Fraud rings targeting this type of fintech count on high fraud rates to hide their activity. With merchants, the variables of small business gaps and eccentricities makes it easy for fraud rings to find gaps to exploit. In this specific case, the merchant onboarder leaned into a looser decisioning process in the spirit of bringing more customers on, faster.

The Indicators

While fraud attacks are expected to be high in the merchant space, the ratio jump of 13 percentage points indicated a coordination and cunning that rang warning bells of a fraud ring attack. Abnormal behavior coming through PC-only traffic was another key marker of a fraud ring afoot. This was likely organized credit card fraud, with a network of criminals using stolen credentials to make unauthorized purchases.

NeuroID Fraud Ring Dashboard View



Large Volume Hides Fraud Spikes

This company has a massive amount of overall volume (green swath and spikes). At first glance, the users flagged as risky seems relatively low.

But upon deeper inspection, this spike shows us there's a fraud ring attack underway. The relatively flat red line shows generalized risky-labeled user activity, with a spike that isn't tremendously high, but is higher than baseline enough to cause concern. If you weren't looking for it, you wouldn't see it—but it's a clear marker of a targeted fraud ring attack.

The Result

With NeuroID alerting to the fraud ring, the merchant onboarder was able to protect against the attempt, which could have resulted in losses of millions of dollars in transaction fraud. Because this company prioritized frictionless onboarding over fraud prevention, they expected a high amount of fraud—but that meant their baseline was so high that jumps sometimes flew under the radar. **Because NeuroID behavioral analytics can calibrate to the specific amount of risk required per customer**, we could cut through the additional fraud noise and call out the alarming fraud ring spikes.

The Takeaway

Automations such as PII-prefill have been broadly accepted as consumer-friendly ways to speed up digital onboarding. But fraudsters are evolving to exploit this in new ways. As more PII data gets exposed—all for the sake of the customer experience—it becomes ever more important for merchants to create holistic fraud controls that aren't solely PII data-dependent and work with vendors able to fine-tune solutions to specific fraud prevention needs.

NeuroID prevented an attempt to defraud **millions in transactions**

100K sleeper fraud ring accounts identified who passed other fraud screening

Proactive detection for **improved loss prevention**

4. Fraud Ring Attack Target: Buy Now, Pay Later Provider

Buy-Now-Pay-Laters (BNPLs) are especially attractive to thin-file credit consumers, such as Gen Z or new-to-country applicants who don't have strong identity verification footprints. This young market of digital natives demand fast and seamless online customer experiences, making a frictionless onboarding process business-critical for growth. But if low-friction also means low-fraud prevention, that could equal lost revenue.

The Attack

This fraud ring was a slow boil, attacking over a three-month span. Stuck between a rock and hard place of friction and fraud, this BNPL was leaning too much toward ensuring good CX—even for fraudsters. And as always, fraud rings found the gaps and burrowed their way in.

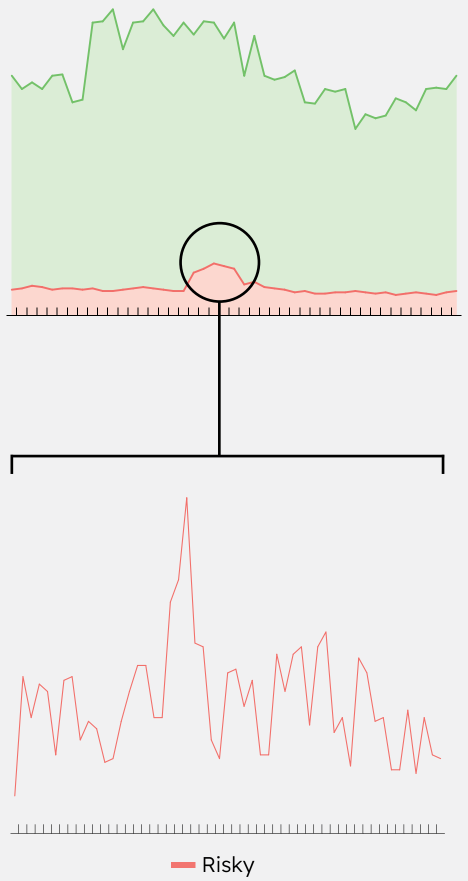
The Indicators

NeuroID was able to correlate the fraud to a high-risk ratio over time and discovered an attack that would have been otherwise missed. Because this was an atypical attack—steadier and more methodical vs. the high-velocity chaos of others we've looked at in this report—the long-term pattern detection was key.

The Result

2,130 applications tied to fraud ring activity were caught over the course of a year, and their potential for immediate and future damage was contained. By utilizing NeuroID behavioral analytics, this customer has been able to keep their high-risk appetite for fraud, while simultaneously closing down fraud vectors and progressively eliminating fraud ring risks.

NeuroID Fraud Ring Dashboard View



Slow-Rolling Fraud Rings

The volume and nature of a business determines how fraud rings try to attack. In this case, it was a slow, methodical approach that tried to fly under the radar, knowing that the high volume of applicants (green swath) would help them avoid detection.

Fortunately, behavioral analytics are impossible to fool. By alerting that these applicants weren't familiar with the inputted PII, the fraud ring was identified.

High-Potential for Damage

With this BNPL, we saw again that high volume combined with a high-risk appetite can camoflauge fraud rings. BNPLs are picking up tremendous momentum in younger applicants and other populations who don't have deep credit histories: fraud rings take advantage of that demographic by attacking in a way that mimics your ideal thin-file applicant.

Once they are in your ecosystem, they can coordinate a sleeper fraud attack and cause way more damage than expected by baseline risk predictions. BNPLs need additional, non-traditional sources of fraud prevention to fight back without hurting genuine applicants.

The Takeaway

Most BNPLs have a fraud check of a one-time password, along with a thorough identity verification. It's common because it works . . . or, used to work. Because of this simple strategy's prevalence in the BNPL industry, fraudsters got good practice in gaming this system over and over and over.

In order to meet the high expectations for customer experience and high-risk for fraud that's inherent to their prime customers, BNPLs should look to multi-faceted fraud prevention at the top of the customer onboarding funnel. Behavioral analytics force fraudsters to self-identify earlier, so the right step ups can be taken at the right time, on the right bad actors.

2,130 fraud ring applications caught by NeuroID

Top-of-funnel signal to identify fraud rings **earlier and more accurately**

Zero friction for genuine applicants

5. Fraud Ring Attack Target: Digital Insurers

As insurance has moved more into the digital world, classic insurance scams have evolved as well. Without in-person human interaction, life insurers often struggle to determine if an applicant actually is who they say they are, while still protecting the user experience from unnecessary identity verification-related friction.

The Attack

This digital insurer had tried identity verification step-up methods. The result was a 10% decrease in genuine applicants due to increased friction, with no noticeable fraud prevention benefits. While the digital insurer was continuing to test the best way to deflect bad actors and streamline good customers, a fraud ring saw their opening.

The Indicators

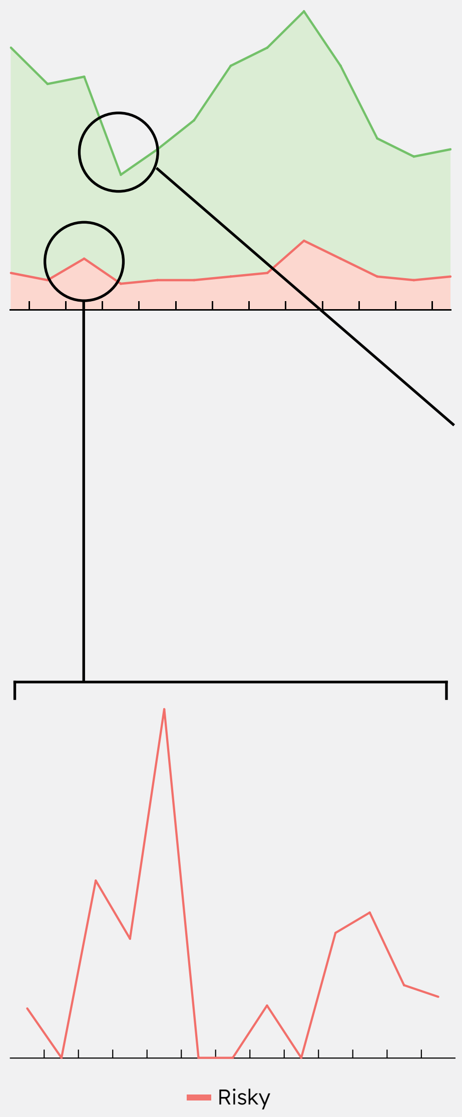
Behavior patterns of high-velocity, inhuman efficiency indicated a likely bot-led fraud ring, with an almost 5x increase in risky tags: up from 2% to nearly 10% in just three days.

The Result

With NeuroID confirming the risky sessions were related to suspicious beneficiary information that all came from one channel, the digital insurer was able to immediately change tactics and stop the attempt with no impact to their customer experience. In this specific case, the digital insurer had been looking for only specific signs to determine whether or not the identity was real—meanwhile the ring was attacking through an untracked methodology.

NeuroID found anomalies that would have been missed and created a composite of all the activity indicators for a more valuable and holistic view going forward.

NeuroID Fraud Ring Dashboard View



Increased Friction Can Reduce Conversions

Blunt force step-up methods can reduce conversions and top-line revenue, sometimes costing more in losses than actual fraud. In this case, you can see how the spike in red is followed by a dip in green: indicating that as the insurer imposed more onerous identity verification steps it hurt conversions, not fraudsters.

All Risk, No Reward

This attack happened during the trial period of NeuroID's behavioral analytics, so we could see just how the step-ups reduced legitimate customers (green swath) with little to no impact on the fraud ring influx. This blunt force step-up of identity verification methods applied to all traffic, potentially costing more in losses than actual fraud.

The Takeaway

Life insurance payouts can be huge. If a 10-member fraud ring gets past detection, that's likely millions paid out to cybercriminals. This is part of why it's a double-edged sword for insurers expanding their digital footprint: as they become more visible, they become more digitally vulnerable.

At the same time, attracting a good customer growth base requires a seamless customer experience. Balancing fraud and friction prevention together is critical for all digital businesses. But this is especially true for digital insurers who have exceedingly high verification needs. The customer journey is a critical competitive differentiator, and incorporating a fraud solution that can streamline decisioning is paramount. An increase in step-up verification, if done improperly, can reduce genuine applicants without deterring fraudsters. Fraud rings might still get through if an insurtech doesn't have the ability to do additional identity pre-screening at scale, ideally prior to application submission.

More holistic view based on NeuroID behavior signals

Reduced friction for legitimate applicants

Increased efficiency and accuracy in step-ups

Behavioral Analytics Unspool Fraud Rings

When a fraud ring is detected, it's tempting to respond with blunt, short-term force. For example, if a fraud ring originated from a specific channel, maybe all activity from that channel is stepped up to manual reviews (or outright declined). These kinds of responses are easy to implement—and easy for fraudsters to overcome. In the end, the losses from false declines can cost more than the fraud ring attack itself.

For every fraud ring detected, there's a more sophisticated version that has evolved and learned from the mistakes of its predecessor. Just like cutting off the head of a hydra makes two more grow back in its place, for every ring you deflect, more rise to the challenge. Successful fraud ring prevention similarly requires a holistic approach, with the right tools to unspool the rings.

NeuroID behavioral analytics provide proactive, passive protection by monitoring crowd-level behavior 24x7 and alerting to shifts that could signal bots or fraud ring attacks. This empowers our customers to make the best choices of who to fast track and who to escalate within their existing fraud stack. NeuroID was built to address the growing need for advanced fraud ring detection within the identity verification world, as these attacks are known to thrive on stolen personally identifiable information (PII). Our behavioral analytics provide a new level of innovation to fill in the massive gaps that digital identity fraudsters take advantage of in traditional PII-reliant fraud stacks.

NeuroID is a frictionless behavioral check that measures how familiar every applicant is with their inputted PII. It analyzes users' behavior as they interact with a digital form or application, looking for scientifically proven tell-tale signs of unfamiliarity. By interpreting these behavioral signals, NeuroID exposes whether users are familiar with the data they've input, which then helps digital companies make real-time decisions on the likelihood that each customer is risky, or trustworthy.

These innovative behavioral analytics are impossible to fake and add no friction to the onboarding process. The result is a fraud prevention solution that seamlessly balances the challenge of friction and fraud while solving for some of the most nefarious and advanced identity spoofing methods that market-leading verification solutions still struggle to detect.

Want to see how behavioral analytics would work in your fraud stack? Contact a NeuroID Fraud Ring Expert today.

neuroID

NeuroID, the global leader in behavioral analytics, 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.