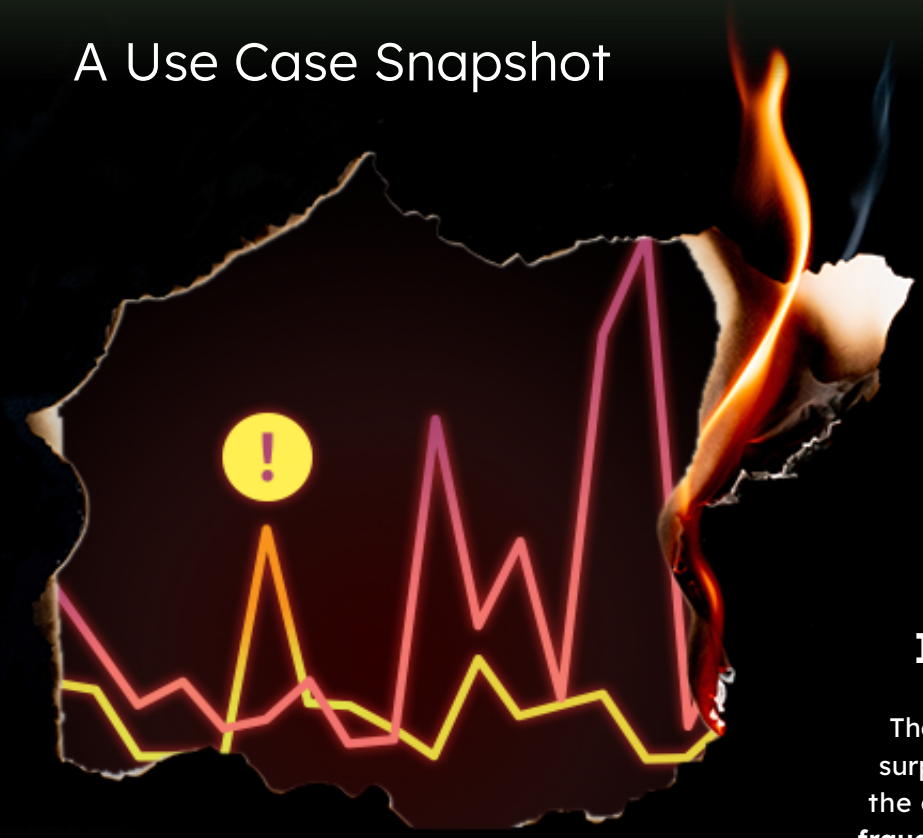
THE LONG-TERM DAMAGE OF SHORT-LIVED FRAUD ATTACKS:

A Use Case Snapshot



NEUROID EMERGING TRENDS REPORTS

17 Customers **5** Months **150** Attacks

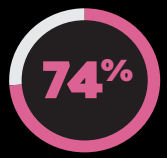
What We Learned & What it Means for You.

Understanding the nature and tactics of today's sophisticated digital identity fraudsters is critical to secure growth and efficient customer onboarding. NeuroID's behavioral analytics solution alerts organizations to potential fraud incidents when an abrupt influx of 'risky' users hits a website. By doing this, we're able to gather industry-unique insights into what these attacks look like, their long-term impacts, and what digital businesses can do to swiftly weed out any fraud that does make it through.

Over a span of five months, NeuroID closely tracked 17 customers' fraud attack patterns. We analyzed the frequency and duration of these cyber-attacks, uncovering insights that could transform how businesses perceive and respond to application spikes.

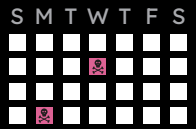
Insights from the Frontline of Fraud

The study showed us two major takeaways: First, about 74% of fraud attacks were surprisingly ephemeral, lasting less than 33 hours. Second, within the five-month period, the customers encountered an average of nine attacks. **That translates to a full-day fraud attack every other week.**



FRAUD ATTACKS LASTED LESS THAN 33 HOURS

WITHIN 5 MONTHS



FULL DAY ATTACK EVERY OTHER WEEK

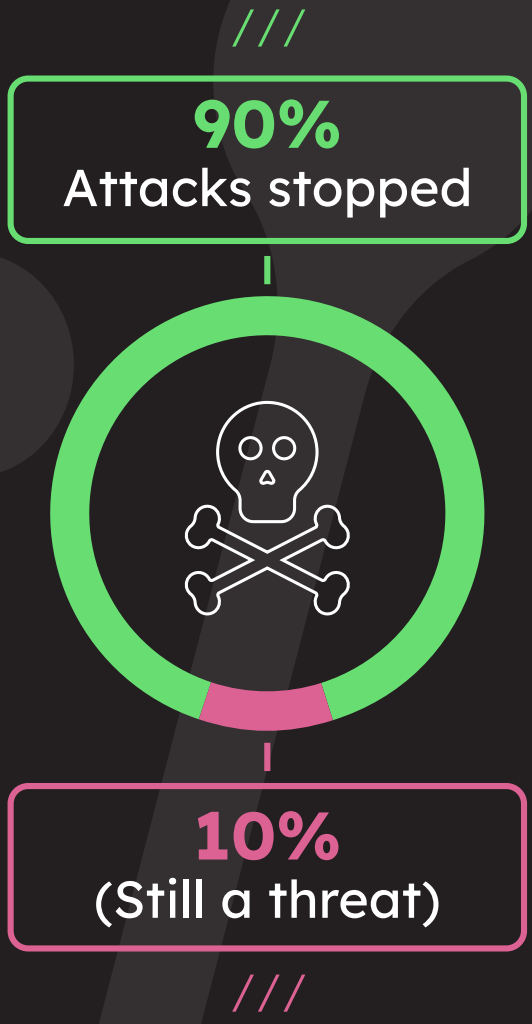
The Big Impact of Short Attacks

These short spikes of risk represent different fraud strategies, likely instances of ambient fraud, a term coined in Alloy's guide on stopping fraud attacks, which refers to a constant level of fraudulent activity that most Financial Institutions (FIs) face. This includes continuous tests by fraudsters on FIs' fraud protection systems for weak spots, as well as small-scale fraudulent
activity from novices and first-person fraudsters. This type of probing is easy to track through behavioral analytics. With NeuroID providing application data monitoring, you can turn the tables on fraudsters and use these probing spikes to identify and patch any potential gaps before bad actors break through (let us show you how).

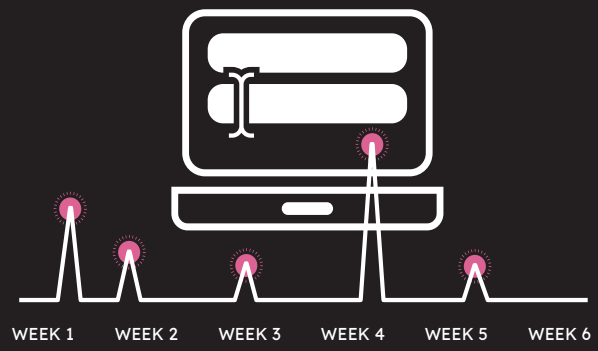
These brief bursts of activity could also signal the onset of Fraud Ring Attacks or High Velocity Attacks. **Fraud Ring Attacks** involve careful precision and patience, with fraudsters testing defenses to inform a broader, more deliberate strategy.

On the flip-side, **High Velocity Attacks** rely on speed and brute force, typically launched by individual fraudsters who've found an exploitable gap. High Velocity Attacks are initiated when a fraudster uncovers a loophole in your fraud defenses and broadcasts this information, often on the Dark Web. This results in a rapid increase in low-quality or clearly risky applications that can overwhelm your defenses. Even if 90% of these applications are stopped, the remaining 10% can still pose a substantial threat due to their sheer volume.

Fraud Ring Attacks and High Velocity Attacks aren't mutually exclusive. Some fraud rings might use stolen identities to launch High Velocity Attacks, while others could disseminate the exploit they used after being thwarted, causing high-velocity attacks against other FIs.



Even if 90% of these applications are stopped, the remaining 10% can still pose a substantial threat due to their sheer volume.



ID Orchestrator identified five unusual spikes in risky activity on the issuer's site, indicating possible application-level fraud attacks. This included more than 500 risky user flags, one-third of whom were being approved by the credit card issuer's other fraud and identity tools.

Behavioral Analytics In Action: A Closer Look

During our comprehensive five-month analysis, we monitored high-level attack patterns to gain insights into overall trends. To see the real impact of those trends, let's focus on one specific attack on a fintech credit card issuer—and how NeuroID's behavioral analytics tools mitigated the risk in real-time.

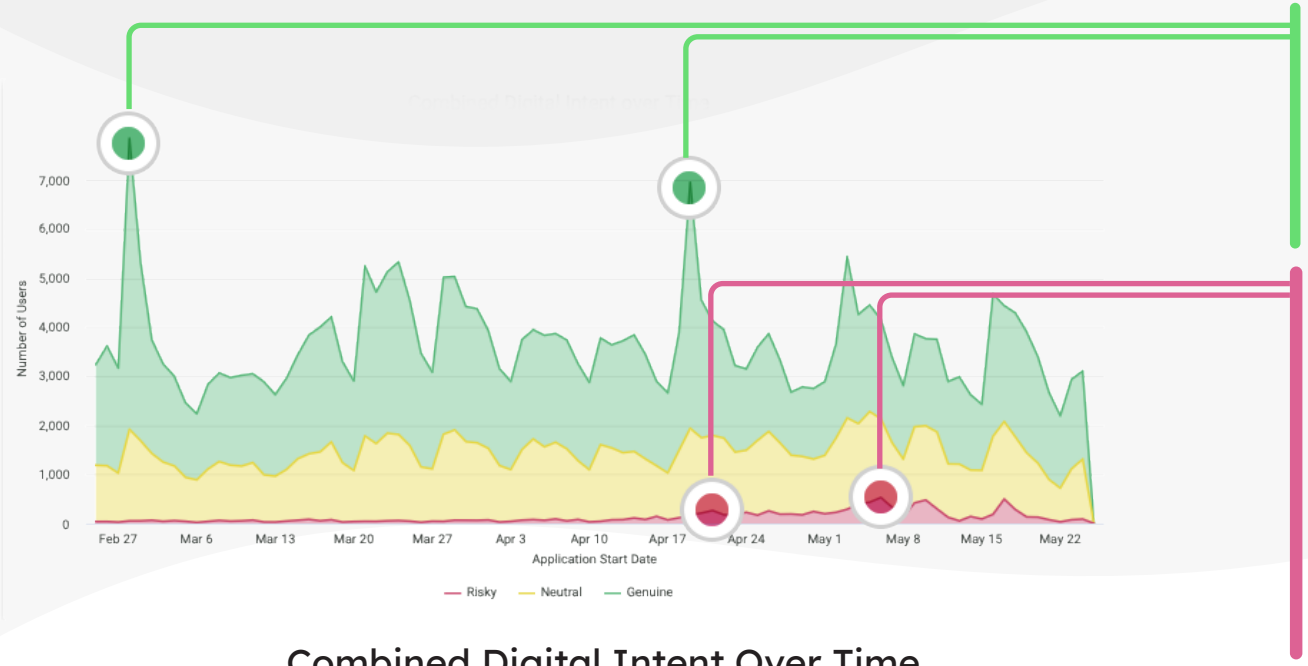
A high-growth credit card issuer integrated NeuroID's ID Orchestrator to detect third-party fraud at both prequalification and customer account application stages. Within a six-week span, ID Orchestrator identified five unusual spikes in risky activity on the issuer's site, indicating possible application-level fraud attacks. This included more than 500 risky user flags, one-third of whom were being approved by the credit card issuer's other fraud and identity tools.

Armed with these results, the credit card issuer escalated the verification process for the flagged applicants to include document verification as an additional step. As a result, many of the risky applicants dropped out. A small subset attempted to proceed and uploaded falsified documents. In addition, many applications that ID Orchestrator classified as risky were later confirmed to have used addresses tied to previously declined or defaulted accounts, which could indicate scams, distributed fraud farms, or stolen identities.

The integration of NeuroID's ID Orchestrator provided the credit card issuer with robust protection against substantial third-party fraud during the application process. By leveraging behavioral analytics' insights, they were able to safeguard operations from fraud that the rest of their tools would not have caught in time.

What Crowd Level Insights Into Application Spike Attacks Look Like In Practice

Looking into a NeuroID dashboard, which visualizes crowd-level applicant traffic separated by their behavior, we see two startling spikes in application quantity.



Combined Digital Intent Over Time

Fortunately, for this bank the spikes are green, meaning the traffic is from genuine users.

Alerted by the spikes, we were able to show that the first increase was due to a successful marketing campaign. When the second spike occurred, it was also the result of a marketing campaign advertising new products. However, the second campaign was followed by this red spike, showing a tagalong group of fraudsters intrigued by the new features and eager to see if they could exploit it. Without NeuroID, they would have flown under the radar and caused havoc.

Preventing the Blitz

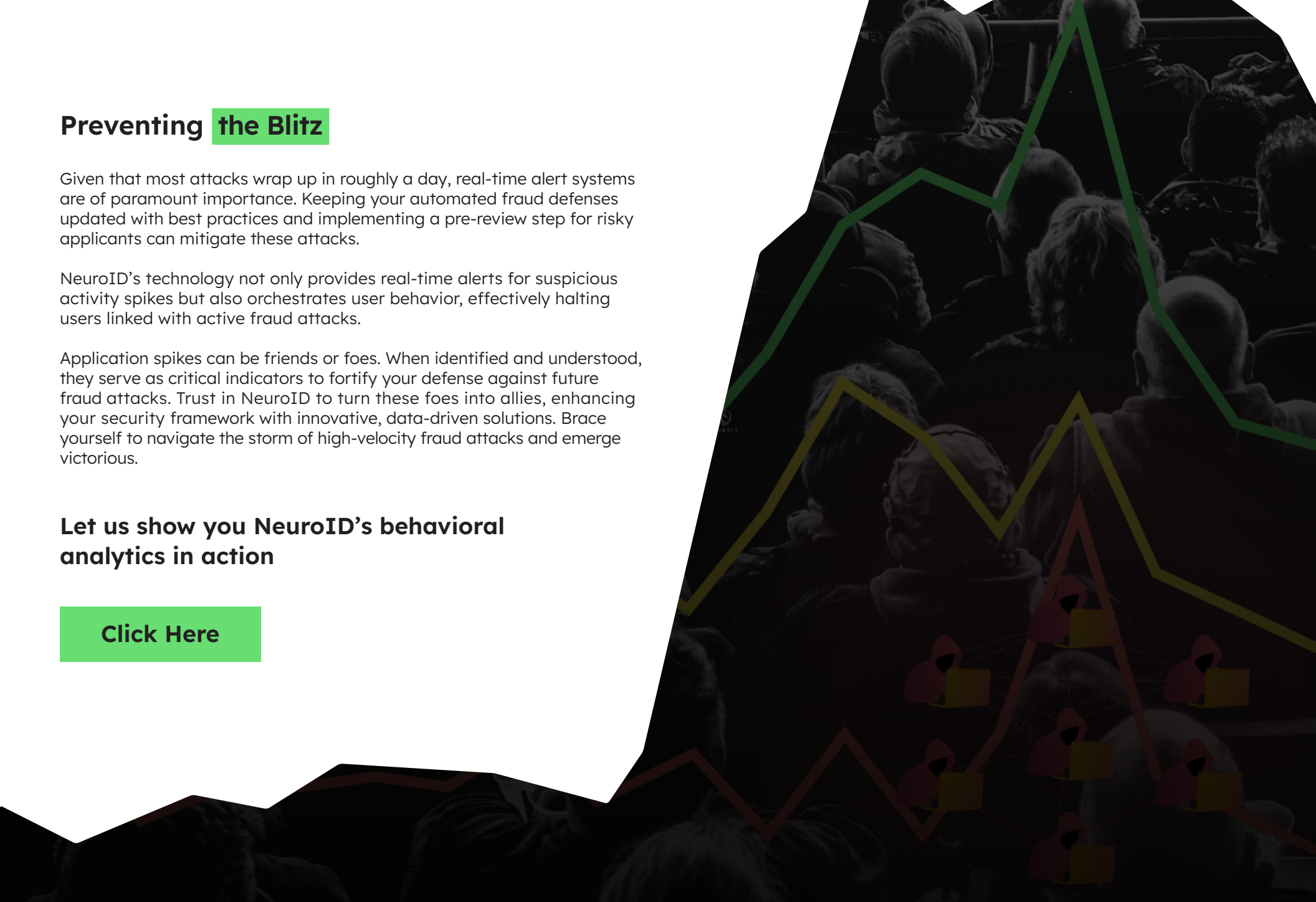
Given that most attacks wrap up in roughly a day, real-time alert systems are of paramount importance. Keeping your automated fraud defenses updated with best practices and implementing a pre-review step for risky applicants can mitigate these attacks.

NeuroID's technology not only provides real-time alerts for suspicious activity spikes but also orchestrates user behavior, effectively halting users linked with active fraud attacks.

Application spikes can be friends or foes. When identified and understood, they serve as critical indicators to fortify your defense against future fraud attacks. Trust in NeuroID to turn these foes into allies, enhancing your security framework with innovative, data-driven solutions. Brace yourself to navigate the storm of high-velocity fraud attacks and emerge victorious.

Let us show you NeuroID's behavioral analytics in action

Click Here



NeuroID's patented behavioral analytics solutions can assess human behavior to determine if applicants are who they say they are. By understanding human digital behavior, fintechs, financial institutions, and all financial companies who do business online can see fraud faster, improve identity-related operating expenses, and more confidently approve genuine customers. Human digital behavior shows how familiar digital users are with the personal information they use to open accounts online without collecting or analyzing any of the PII itself. Visit **Neuro-ID.com** to learn more.