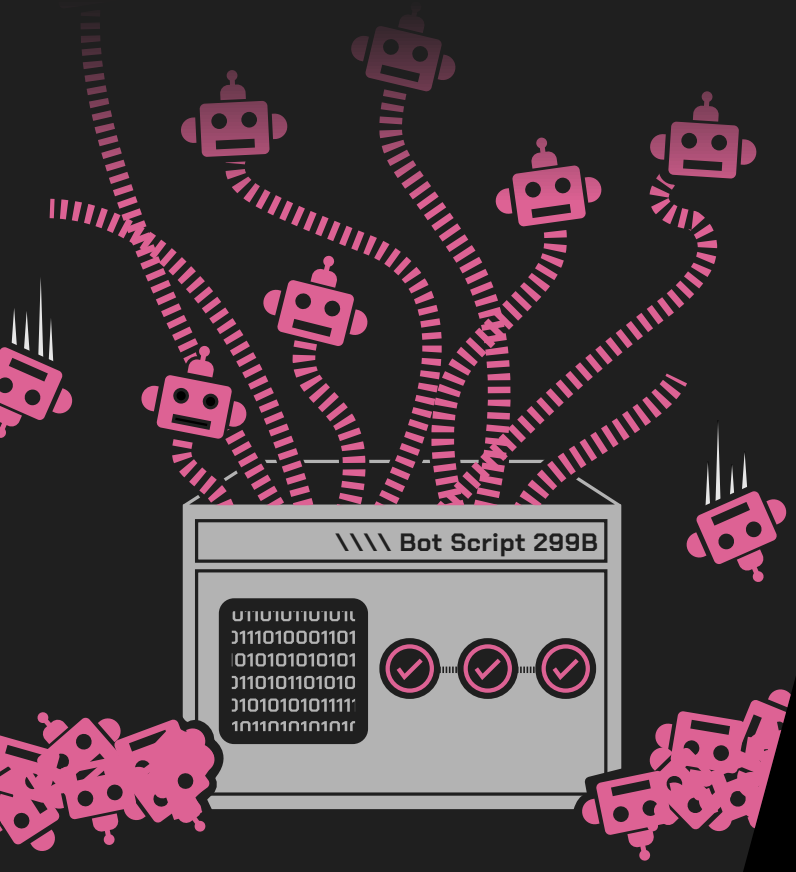
EMERGING TRENDS IN BOT ATTACKS:

A Use Case Snapshot



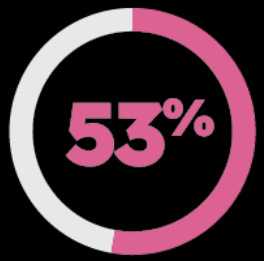
EMERGING TRENDS IN FRAUD SERIES EDITION 2

15 Customers | **4** Months | **98%** Accuracy

What We Learned & What it Means for You.

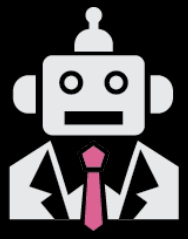
Understanding the nature and tactics of today's sophisticated digital identity fraudsters is critical to secure growth and efficient customer onboarding. NeuroID's behavioral analytics solution alerts organizations to potential fraud incidents when an abrupt influx of 'risky' users hits a website. By 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 four months, NeuroID closely tracked 15 customers' bot attack patterns. We analyzed the frequency and duration of these cyber-attacks, uncovering insights that could transform how businesses perceive and respond to bot attacks (we also have significant data on the impact of application spike attacks from another study—read ***The Crowd Goes Wild Edition 1: The Long-Term Damage of Short-Term Fraud Attacks*** for more).



OF CUSTOMERS ATTACKED BY BOTS

OF BOT ATTACKS WERE FIRST SIGNALED BY HUMAN PROBES



BESPOKE BOT BLITZES TAILORED TO SPECIFIC FRAUD CONTROLS

Insights from the Frontline of Fraud

In this customer study sample, NeuroID behavioral analytics acted as part of the first line of defense in a fraud stack. By monitoring the crowd-level trends at the top of the customer onboarding journey, we reached several key findings.

Bot blitzes are pervasive

In the four-month study period, a staggering 53% of NeuroID customers who triggered alerts had a bot attack.

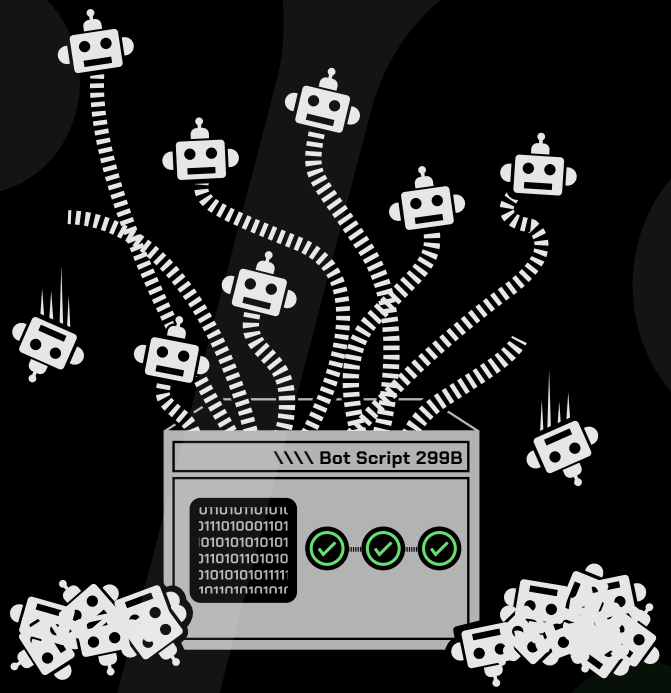
Bot attacks are meticulously tailored to your defenses

The bot assaults included a sophisticated division of labor—100% of observed botattacks were set up by human-testing beforehand. For example, with one customer we tracked how human fraudsters carefully probed fraud defenses, inputting dummy data in order to expose fraud controls. They then programmed bots to get around those specific controls and exploit any vulnerabilities. These are not indiscriminate mass-bot-attacks on any target; they are meticulously tailored to bypass specific customers' unique control mechanisms.

Bots attacks are cyber-hydras

Cut off the head of one bot attack and two more grow back in its place. We saw in real-time how even as NeuroID customers tightened controls to stop one attack, bots targeted another product onboarding session with different controls. This told us that fraudsters were aware of multiple points of entry and even planned ahead to strategically move across them all. Our customer had to play a high-stakes game of whack-a-mole across their customer onboarding journey to stay ahead of fraudsters (which NeuroID helped solve—keep reading for the details).

Here's more on what we learned from these attempted attacks and the emerging bot trends we're keeping an eye on.



Cut off the head of one bot attack and another grows in its place.

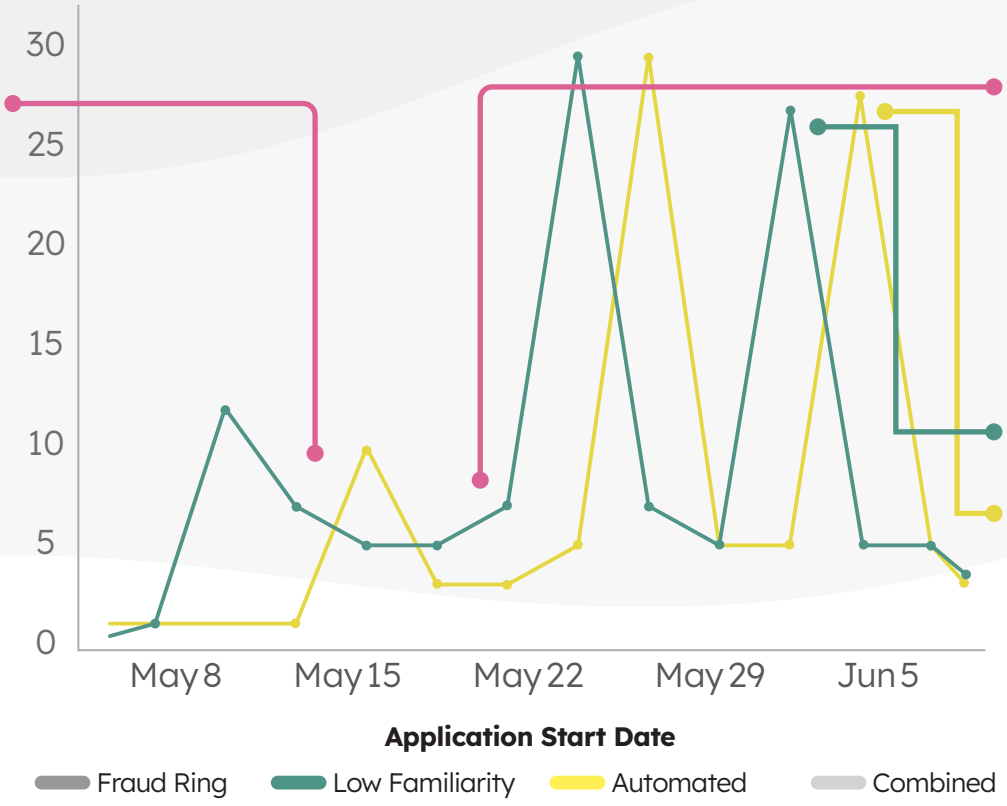
Overpowering the Bot Onslaught: What to Do When Half Your Applicants Are Bots

NeuroID behavioral analytics picked up a bot surge across a consumer financial manager's digital application process.

Risky Users, Separated by Type of Risky Behavior

1. Initial attack being set-up

We noticed a pattern: each one started with a human fraudster testing for weakness, followed by a probe of bots, leading finally to a flood of bots that lasted for two weeks.



2. Full-blown attack, alternating human v bot

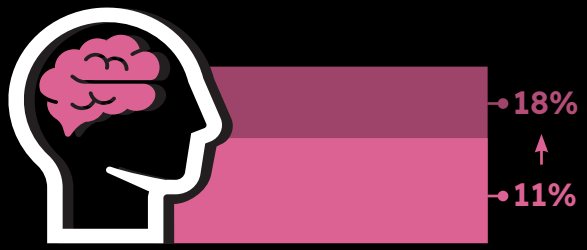
The set-up pattern of humans ahead of bots became clear, as the fraud-pair worked in tandem toward the huge spike onslaught.

Human

Bot

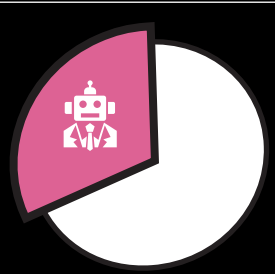
During that week, 50% of all their traffic was labeled as bot: **nearly triple the bot attack volume** compared to the company's average baseline.

Was it a bot script that fraud tools weren't equipped to mitigate? Was it human intervention combined with bot speed? The end result was the same: fraudsters were making it past traditional verifications and wouldn't have been caught without the power of behavioral analytics.



Risky Human Activity Metric jumped from 11% to 18% over a 3 week time span

One bad actor was linked to 22 merchant tokens from the same browser



31% of the total user population for the day were bots

Bots on the Prowl: By the Time You See Them, It's Already Too Late

In another use case, NeuroID identified a spike in suspicious activity on the account sign-up page of one of our payment processor customers. This wasn't just any unusual activity: there was a two-fold uptick with an increase in both human users and bots, with our risky human activity metric jumping from 11% to 18% over the span of just 3 weeks.

What caught our behavioral model's attention was that most of these risky human users were adeptly completing the platform's application forms at an outlandish pace and sailing through business and personal information markers. For example, one bad actor was linked to 22 merchant tokens coming from the same browser. Heavy use of the 'paste' command in email and name fields also raised additional behavioral alarms. This all suggested a premeditated set-up: could these humans be paving the road for bots to race in at scale, overcoming all speed-bumps?

Looking closer, we saw a substantial surge in automated users that day, comprising 31% of the total user population for this payment processor. It was clear these bots weren't completing applications on their own, but were successfully navigating through complex sign-ups, suggesting they might be capturing credential information or probing email associations, possibly using scripts already put in place by that first-wave of risky human operatives.

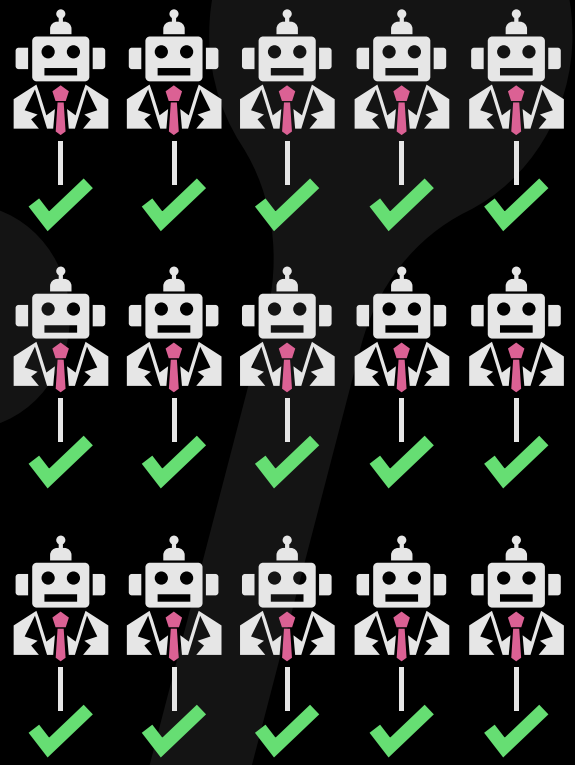
But the payment processor didn't experience a fraud attack—the bots were instead likely working to note what credentials got them through account set-up and storing that information for a future blitz. In this case, the human-bot fraudster collaboration was working to learn the system for a future full-scale onslaught. We know that if bots are on a site, it's always a problem: either they're testing for vulnerabilities or acting on what they've already learned. With behavioral analytics, this payment processor was able to learn the human-bot patterns even as they tested and prepared to stop any future attack before it starts.

Another distinguishing attack within our bot study was the lightning-fast pace of data entry for one targeted customer, with text entered into fields in less than a tenth of a second and an entire session lasting under a minute. NeuroID models are trained to look for this kind of behavioral input and respond with alerts that our customers then use to make decisions. In this case, of the risky users detected, 1600+ were automated, with a staggering 99% of them completing applications and signing up. It was clear that the bots were thwarting identity verification step-ups and getting ready to wreak havoc.

Among the bot session speed frenzy, there was a singular validation step that was expected to stop these exact types of attacks: when the applicant must complete a phone verification. The session logs indicated that at this step, the automated script paused and the application window was switched, possibly for the retrieval of a one-time pin from an alternate source before resuming and completing the session at full, inhuman speed. The data entered was correct and would have been enough to move through PII-based controls—but the hidden trail of behavioral analytics gave it away.

NeuroID's ID Crowd Alert™: A Powerful Tool in the Fight Against Evolving Bot Strategies

The potential of human users scripting bot attacks is alarming, and should be a wake-up call for any digital business. At NeuroID, we are not just detecting bots or risky users; we're uncovering the correlation between them. The increasing sophistication and agility of new attack trends underline the importance of vigilance and advanced threat detection.



In this case, of the risky users detected, 1600+ were automated, with a staggering 99% of them completing applications and signing up. It was clear that the bots were thwarting identity verification step-ups and getting ready to wreak havoc.

Our bot indicator behavioral analytics enable our customers to take meaningful action quickly to eliminate bots, wherever and however they attack.

But a new human-bot collaboration wasn't the only alarming new trend we found. Our study of attack attempt trends showed a surprisingly significant proportion of bots operating from mobile phones—behavior that we haven't previously seen in this style of attack. This could be indicative of a new wave where bots' modus operandi is evolving to even better mimic human behavior, or a hybrid of the human-bot connection—it's something that we are keeping an eye on, and that our crowd-alert models are uniquely situated to solve. We have 98% precision with our bot indicator behavioral analytics, enabling our customers to take meaningful action quickly to eliminate bots, wherever and however they attack. As bots are getting more sophisticated, our broad, multi-tier approach is key to detecting them at every point of entry.

Bot Behavior and Your Bottom-Line

In the course of our bot behavior analysis, we also noted that while both genuine and fraudulent sessions primarily originated from PC devices, there was a significant difference in success: for one customer, 99% of fraudulent bot sessions completed the application process, compared to just 67% of genuine users. This tells us that it's sometimes easier for fraudsters to get into a business's ecosystem than for actual revenue-driving customers to onboard: the very friction built to deter fraud is no match for their determination. Bots are often more dedicated than your genuine customers, who have the opportunity to window shop and leave onboarding if it's too complex. Unlike genuine customers, fraudsters have a focused and determined drive to get into your business, overcoming any step-ups or friction you put in place to keep them out (friction that might instead cost genuine customers).

Without adding friction to the onboarding process, NeuroID's ID Crowd Alert tracks the number of risky users coming to an application and alerts to abnormal spikes.

This could be as simple as unfamiliarity with their first name or unexpected typos in their mailing address. Looking at crowd-level patterns, we track specific behaviors that have proven to be associated with bot activity. NeuroID provides dashboard visualizations that show traffic by risk, origination, and what fraud checks these risky users have already passed through. With this data, our customers can make highly informed decisions on how to flip those numbers, so it's more likely that 99% of genuine, life-time value-generating customers make it through the application process—not fraudsters.

The emerging patterns of targeted bot attack strategies across multi-vector vulnerabilities is deeply concerning. Protecting revenue and fraud risk is not just about detecting bots or risky users independently; it's about connecting the crowd trends to predict and assess all factors, and how one might indicate the other. The evolution, speed, and agility of bots in navigating applications are a stark reminder of the need for vigilance and solutions that cover the crowd, not single-points of access or PII-based checks.

Outsmart the bots.

Contact NeuroID to see behavioral analytics in action.

Click Here

The end result was the same:

Fraudsters were making it past traditional verifications and wouldn't have been caught without the power of behavioral analytics.

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.