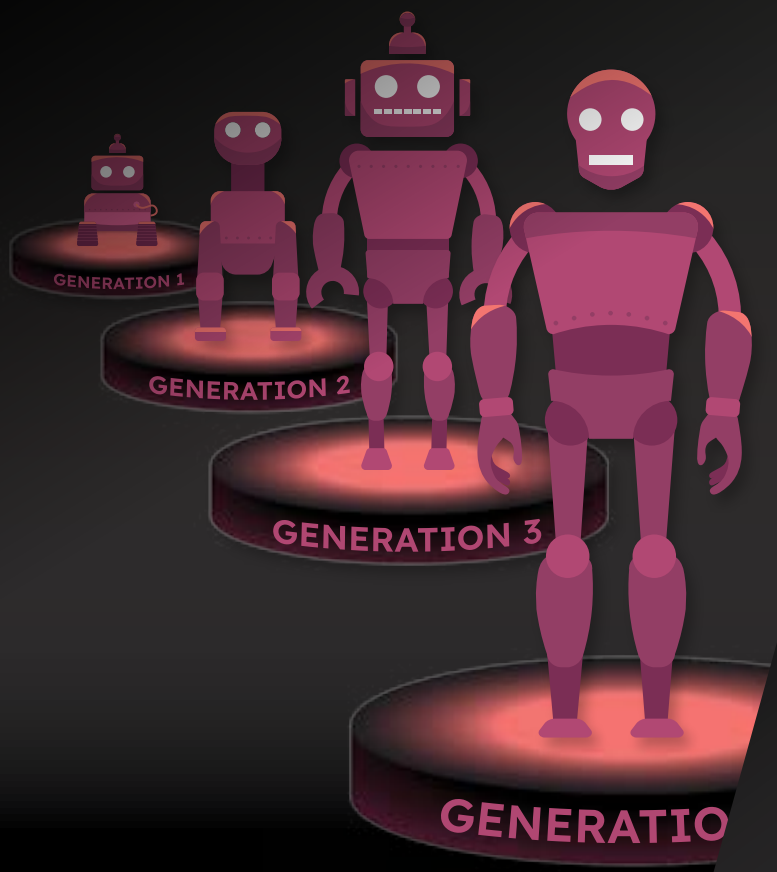
FIGHTING THE FUTURE OF FRAUD:

Understanding and Combating Next-Gen Bots



EMERGING TRENDS IN FRAUD SERIES EDITION 4

Bots are the scourge of fraud teams, constantly nibbling through holes in fraud stacks. Fraud teams try to build better mouse traps to stay ahead, and bots, in turn, learn and adapt. But these mice aren't just avoiding mousetraps. They reverse engineer the traps into stepping stones towards their next evolution.

Go to any digital financial services' fraud team, and you'll find a standard set of fraud tools. It's a maze of step-ups and checks to stop ever-advancing fraud techniques—but this best-practices group of tools gives genAI and machine learning bots a perfect testing ground. They can trip the traps, poke the holes, and adapt workarounds for almost any mousetrap put in place by even the most vigilant fraud team.

As one of the most advanced defenses against bots,[4] behavioral analytics is the mousetrap that fraudsters most want to defeat. That's because behavioral analytics is built on user behavior patterns that are so nuanced, bots haven't been able to replicate them—until now. **As bots have evolved, they've learned to incorporate the human-like behavior that distinguishes bad bots from good users.**

43%

of NeuroID customers attacked by bots were hit by next-generation bots almost exclusively[1]

11%

of traffic in 48 hours was bots for one top bank—an increasingly common surge of focused attacks[2]

10%

rise in automated ATO attacks in 2023[3]

1. Based on a study of NeuroID customers analyzing bot encounters over a 7-week window
2. Based on a study of NeuroID customers analyzing bot encounters over a 7-week window
3. "Yes, The Bots Really Are Taking Over The Internet," Forbes 2024
4. *Emerging Trends in Bot Attacks: Insights from the Frontline of Fraud*, 2023

Insights From the Frontline of Fraud

Where does that leave behavioral analytics, which was built on defining and identifying signs of genuine human behavior? **And more importantly, where does it leave NeuroID customers, who need bot protection more than ever as the infestation only continues to grow?**

Those are the questions our data science team set out to answer. They built a new model to detect these stealthy, human-like bot features and analyzed how prevalent next-generation bots had become. In an analysis of our customer data across a 7-week window, we came to four primary conclusions:

1. **Today's attacks are made up of not just more sophisticated bots but higher bot-volume than ever before.** 71% of our customers experienced bot attacks in that 7-week timeframe. Bots have been making up more and more of the attacks—in June 2024, bots led 2x the number of attacks than they did in January 2024.

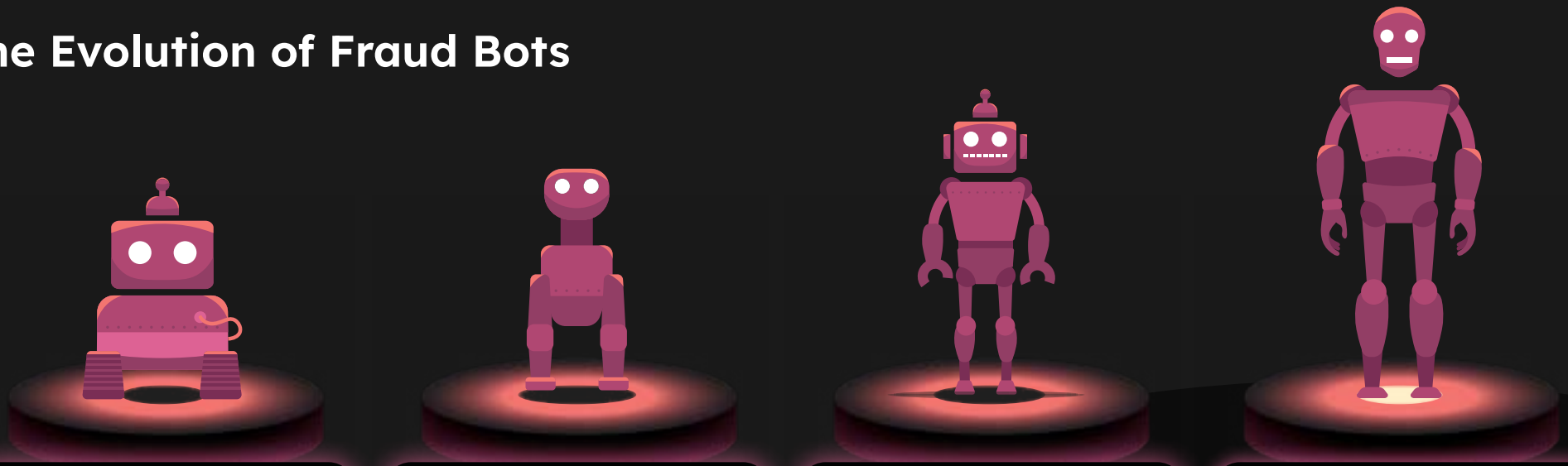
2. **Advanced, fourth-generation bots are far more prevalent than expected.** For almost 50% of our customers who encountered bots during the analysis, more than 95% of the bots were next-generation. These fourth-generation bots are designed to bypass behavioral analytics by mimicking human behaviors, such as typing speed and mouse movements, making them harder to detect at entry.

3. **Fintech and sub-verticals are attracting more bots than ever—but every business is a target.** While financial products with easy sign-ups (such as payment platforms) are typically the jewel of a bot-writing fraudster's eye, more and more banks and lenders are attracting huge swaths of bots. In our 7-week study, top banks and large lenders had more than 3% of their traffic flagged as bots. Bots are everywhere, targeting everyone.

4. **Because bots are overcoming today's fraud mousetraps, NeuroID is critical to next-generation detection.** First- and third-generation bots are still in heavy rotation for fraud attacks, and the fourth generation isn't going anywhere even as the fifth generation is on the horizon. The generations build on each other, which means your solutions need to evolve similarly. For more on why NeuroID is mission-critical to stopping all bots, go to page 6.

> [Bot-related] Account takeover (ATO) attacks rose by 10% in 2023, with 44% targeting API endpoints, compared with 35% in 2022.
>
> In fact, of all login attempts across the internet, 11% were associated with ATO.
>
> The worst-hit industries were financial services at 37%.
>
> - *Yes, The Bots Really Are Taking Over the Internet*, Forbes 2024

The Evolution of Fraud Bots



First-Generation Bots

Simple, basic scripting that made cURL-like requests to websites using a limited number of IP addresses

Strengths

Scraping, carding, and form spam

Weaknesses

Easy to detect and block through IP blocklisting and user-agent analysis because they couldn't store cookies or execute JavaScript

Second-Generation Bots

Used headless browsers like PhantomJS and later versions of Chrome and Firefox in headless mode. Can maintain cookies and execute JavaScript, making them more capable than Gen 1.

Strengths

Application DDoS attacks, scraping, form spam, skewed analytics, and ad fraud

Weaknesses

Easy to detect through browser and device characteristics analysis and behavioral patterns across websites

Third-Generation Bots

Operated through full-fledged browsers, either dedicated or hijacked by malware. They could simulate basic human interactions, such as mouse movements and keystrokes, but lacked human-like randomness.

Strengths

Account takeover, application DDoS, API abuse, carding, and ad fraud

Weaknesses

Detected through behavioral analysis that can identify programmatic sequences in their actions

Fourth-Generation Bots

Exhibit advanced human-like interactions, such as moving the mouse in random, human-like patterns and changing user agents while rotating through thousands of IP addresses. These bots often employ "behavior hijacking," recording real user interactions to closely mimic human behavior

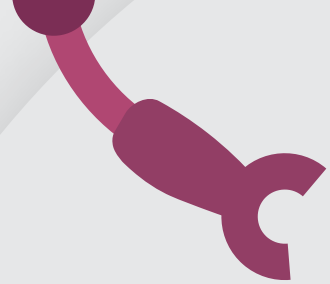
Strengths

Account takeover, application DDoS, API abuse, carding, and ad fraud

Weaknesses

Mitigating these bots necessitates machine learning-based technologies, such as intent-based deep behavioral analysis (IDBA), which can detect these sophisticated bots with high precision

Bot generational markers first defined by Radware



> The business models of crime-as-a-service, phishing-as-a-service, and ransomware-as-a-service continue to **lower the barrier of entry** for new and less technologically proficient cybercriminals, facilitating more online fraud and enabling threat actors to conduct more sophisticated fraud campaigns.
>
> *-Interpol Global Financial Fraud Assessment*, May 2024

Are Fourth-Generation Bots Really Worse Than the Previous Generations?

Bots weren't always this bad. First-generation bots are now easily identified by their speed and lack of errors. Second- and third-generation bots evolved more sophisticated automation than their first-generation predecessors, including headless browsers and malware that defeats any device or browser characteristic checks. But they still lacked the minute behavioral markers indicating a real person behind the screen.

Today, fourth-generation bots can mimic human actions almost perfectly, bypassing traditional fraud detection at every level.

Bots don't evolve in a linear thread with each previous version sunsetting as the new one takes hold. Fraudsters deploy different bots in different ways for different purposes (and sometimes in hybrid combinations with humans[5]). Your mousetrap needs to catch all generations at all times without being overengineered to the point of data deluge.[6]

This means that adding new technologies, such as behavioral analytics, is critical for detecting next-generation bots. But at the same time, device and network intelligence remain essential to finding the first- and second-generation bots that aren't going away any time soon. After all, fraudsters will always choose the easiest path forward—why use a fourth-gen bot when a first-gen bot will do?

5. Emerging Trends in Bot Attacks: Insights from the Frontline of Fraud, NeuroID 2023
6. How Overengineered Fraud Stacks Underperform , NeuroID 2023

Hyper-Efficient Fraud: The Impact of GenAI

In addition to those challenges of keeping up with the pace of bot evolution, genAI lowers the barrier of entry and makes it faster and easier to deploy bots. Two years ago, you'd need an advanced education in JavaScript or Python to create a fraud bot. With genAI, log on to FraudGPT and you're done in seconds: anyone can efficiently generate code and fake identities at scale.[7]

In addition to genAI, the rise of "bot-as-a-service" has also made bots accessible to anyone, even those with limited technical skills or desire to use the genAI basics. Any citizen fraudster can use these pre-built tools for everything from account opening and credential stuffing fraud to phishing and malware attacks.[8] Or they can outsource it—"fraud-as-a-service" is another growing trend, where cybercriminals who lack the technological proficiency to pull off attacks can outsource their work, or simply deploy it at scale through fraud farms.[9]

This hyper-efficiency has made the most lucrative fraud styles, such as synthetic identity fraud (SIF), much easier and more attractive to fraudsters at every level. SIF was already the fastest-growing type of digital fraud, increasing by 6.1% globally from 2022 to 2023 and 184% from 2019 to 2023. With the hyper-scaling enabled by sophisticated bots, SIF now comprises 85% of all fraud in the US.[10]

Combine easy-to-access technology with genAI, and bots are now evolving at lightning speed. The future of fraud bots has just begun.

> Bots have transitioned from standard scripts, then utilizing hybrid approaches, and now embracing periodic advancements thanks to easily accessible AI technology such as ChatGPT. This evolution is happening every six to twelve months.
>
> - *AI-enabled future crime,* Crime Science Journal

7. How GenAI Supercharges Fraud—and How to Fight Back, NeuroID 2023
8. The Anatomy of a Fraud Ring, NeuroID 2022
9. "Fraud as a Service: An Emerging Threat in the Cyberlandscape," The Paypers, 2023
10. *5 Fraud Forecasts: What We Got Right and Wrong in 2024 (So Far)*, 2024

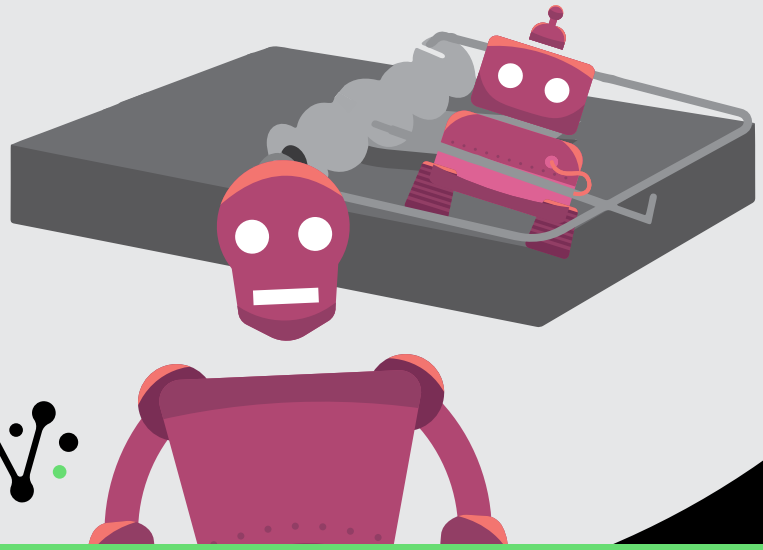
How Bots are Beating Behavior

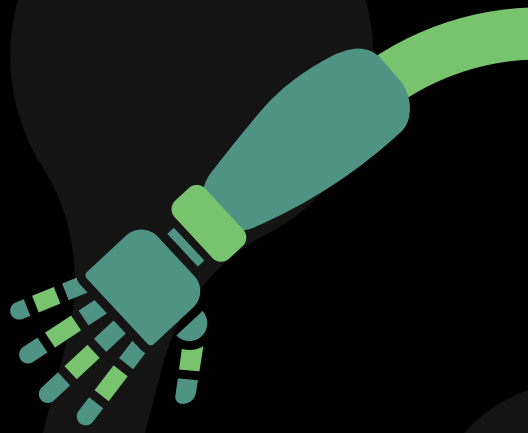
(and Every Other Fraud Detection Technique)

Historically, bot detection has relied on tools like IP blocklisting, user-agent analysis, and simple behavioral heuristics. These methods were effective against the first generations of bots, which used predictable, non-human patterns. But as bot detection methods improved, so did bots' evasive maneuvers. Not only that, bots realized which tools were most effective in defeating them and turned their generative learning skills towards specifically overcoming them.

Fourth-generation bots mimic human behavior almost perfectly. For example, they know to move a mouse randomly, not in the predictable straight lines that gave away their grandfather bots. They rotate through thousands of IP addresses while changing user agent strings, and mobile emulators extend fourth-generation bot capabilities beyond browsers. Fourth-generation bots can even perform genuine user behavior "hijacks," where they record swipe and mouse patterns, hover times, and pressure levels on icons, among other behavioral tells, and incorporate them into their own performance.

The mousetraps we built to defeat the mice are being weaponized against us.





Bot attacks often result in downtime, increased server load, and drive higher operational costs. In 2023, digital companies reported **an average of 25% increase in costs related to mitigating bot-related incidents**, according to the Identity Theft Resource Center *Trends in Identity Report*

Case Study Snapshot: A Better Bot-trap

A NeuroID top bank customer had a huge bot attack. How did the NeuroID behavioral analytics bot signal work against hyper-advanced bots?

A top bank identified a fraud attack through an anomalous increase in daily application volume—several thousand high-risk applications within a week.

With no fraud vendor alerting them to a possible attack (or flagging the several thousand identified fraudsters), they struggled to understand what the fraudsters could have done that made their applications look so normal.

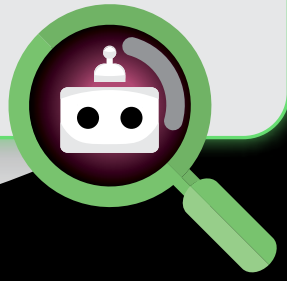
NeuroID investigated the attack and discovered they were led by highly sophisticated, next-generation bots that no other vendor was trained to catch.

Once NeuroID analyzed the bank's data further, we discovered an additional 20K fourth-generation bots for a total attack of almost 25K high-risk applications during a 4-week period.

The bank upgraded to NeuroID's V2 bot signal within a week following the investigation outcome, realizing the impact of fourth-generation bots and the power of the NeuroID.

NeuroID V2 Bot Signal Caught

99.8% of All First-Generation Through Fourth-Generation Bots



Additional Results from Customer Bot Tests Across 7-Week Period

Top 10 P&C Insurer: Caught 21K fourth-generation bots that made up roughly 25% of total bot traffic during the timeframe

Consumer Finance Platform: Caught 14K next-generation bots that made up 75% of total bot traffic during the timeframe

Payment Processor: Caught 88K next-generation bots that made up roughly 50% of total bot traffic during the timeframe

Top 20 Bank: Caught 4K next-generation bots that made up roughly 98% of total bot traffic during the timeframe

A Literal Bot Mousetrap

As a further dive into the sophistication of our V2 bot signals, let's look at one specific example: **mousing patterns.**

When building NeuroID behavioral analytics V1 bot signals, one of the most basic bot giveaways was mouse movements. Instead of the typical fluid motion of a human-controlled mouse, bots generate singular points in space where the mouse clicks.

NeuroID V1 bot signal logic was implemented to detect these patterns and even differentiate the subtleties of human or non-human mousing, where human-mouse movement naturally resembled bots due to the touch, taps, and clicks.

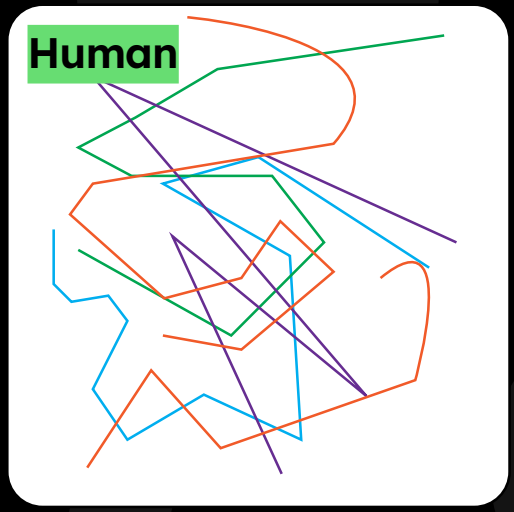
Enter the Fourth-Generation Bots

With fourth-generation bots, navigation has evolved to be much more human-like. But still, unlike the typical erratic motion of humans, our data science team noticed subtle behaviors, which are discrete signs of a bot or script.

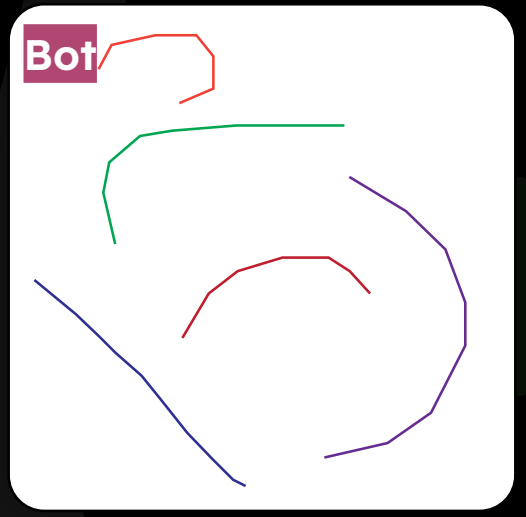
So, the bots evolved. But so did our signals. For mousing, NeuroID data scientists developed algorithms that identify the difference between smoothing an already smooth trajectory vs. smoothing a wiggly, natural trajectory. One results in noticeable bot giveaways.

It's these kinds of small distinctions that create our signal's accuracy in identifying all bot activity, across all generations. These details, expanded and embedded into every level of behavioral interaction, have enabled us to address autofillers, transition times, and other minuscule behavioral secrets that bots evolve to defeat. This iterative process works because it's built on an extensive corpus of our bot data. Genuine user behavior data vs. bot data can be compared in innumerable ways, iterated on, and made into better mousetraps even faster than the bots can reconfigure them. A somewhat sophisticated bot will run a script that looks the same as humans: slower typing speed, human-like mouse movements, and behaviorally accurate transitions. But more sophisticated bots begin to break that pattern, and run the bots differently each time. Fortunately, our analytics cover it all.

Mouse Movements:

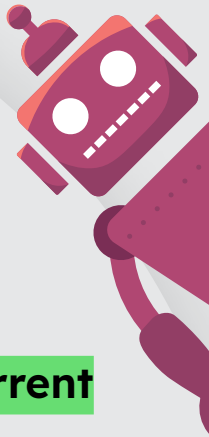


Humans navigate form fields in a chaotic and random way.



Bots recreate the pattern but without the randomness. Their navigation creates smooth lines.

> Bad bots interact with applications in a way that mimics legitimate users, **making them more challenging to detect and block.**
>
> They exploit business logic by exploiting an application's intended functionality and processes rather than its technical vulnerabilities.
>
> *- 2024 Bad Bot Report,* Imperva



From Bot-Trap to Bot-Deterrent

The amount of signals that NeuroID collects requires fraudsters to advance heavily to respond. We're just seeing the tip of the iceberg in terms of fraudster innovation with new technology. But at the same time, fraudsters are still making money with less sophisticated schemes. From a fraudsters' perspective, *if it ain't broke, don't fix it.* **Fraudsters won't increase attack complexity for the same monetization.** They don't need to make things more complicated if they can get in with old-fashioned synthetic identity theft. They work at scale, and efficiency is key.

The flip side to that is they will hyperfocus on the laggards who don't have sophisticated bot prevention and squeeze all the juice they can out of them, so they don't have to launch sophisticated attacks that take more effort. It's like a mouse smelling some cheese through an open window. They're going to go for the house that left the window open over the one where they have to gnaw through the walls. This is why a layered fraud fusion approach that adds advanced bot behavior signals to device and network intelligence is so vital. It doesn't just stop singular attacks, but it drives them away toward others who don't have that same level of protection.

The Future of Fraud: Preparing for Next-Gen Bots

The rapid evolution from first-gen to today's fourth-gen bots has made many traditional fraud protection tools ineffective. If first-gen bots were Roombas, these fourth-Gen bots are Rosey the Robot, the Jetsons' android maid: hyper-efficient, multi-purpose, and nearly human.

Because NeuroID specializes in bot detection, we've noticed changing bot trends and talked to many industry leaders about this shift for a while. We've seen new hybrid bot-human attack strategies take center stage[11], and how today's bots, enhanced by genAI, can easily bypass previously effective detection tools (sometimes making onboarding easier for bots than for real humans).[12]

Hyper-advanced bots—and bots who continue to rise in sophistication—are the new normal. And these bots are attack-agnostic: while it was previously thought that sophisticated bots targeted only high-profile companies, every NeuroID customer with bot activity over the 7-week study had some form of fourth-generation bots. This was true across all installations, with the V2 bot signal detecting advanced bots where every other solution in a fraud stack failed.

NeuroID's continuous evolution in bot mousetraps through behavioral analytics makes it increasingly difficult for fraudsters to succeed. As a result, they're incentivized to target less fortified systems, making organizations without NeuroID's detection more vulnerable. In an era of rapid technological advancement, our adaptive bot signals and strategies ensure robust protection against the ever-growing threat of advanced bots.

We've always been and always will be specialists in stopping bot-attacks, no matter the bot generation. **NeuroID's multi-dimensional approach uses behavioral analytics and device/network signals to achieve 98% accuracy in bot detection.** We're continuing to innovate to detect ever-more sophisticated bots and help you stay ahead of every bot evolution that comes next.

About our Analysis
- 7-week window spanning April 24 – June 11, 2024
- Included over 55 US Credit Unions, Insurers, Lenders, Credit Card Issuers, Banks, Fintechs including Payment Processors, Platforms and Consumer Finance platforms who are current customers of NeuroID with our bot signal in place.

> **In the past 12 months alone, the sophistication of bots has roughly doubled, and the advent of tools like generative AI will only accelerate their rate of advancement. The more sophisticated these bots become, the more difficult they are to stop.**
>
> *- Bad Bots are Growing in volume and Sophistication—Here's What to Do About It,*

NeuroID combines the power of industry-leading behavioral analytics with next-gen device intelligence to secure your entire user lifecycle, starting with the very first interaction. The only solution to combine the power of behavior and device, our unique approach identifies invisible fraud from day one. NeuroID's real-time, pre-submit fraud alerts, coupled with industry-specific best practices, empowers organizations to refine their fraud detection strategies for more precise outcomes with zero friction.

11. *Emerging Trends in Bot Attacks: Insights from the Frontline of Fraud*, 2023
12. *Timeline of a Bot Attack*, 2023