neuroID
A part of experian.

How a Top 5 Bank Optimized Their Fraud Stack and Stopped Evolving Attacks with NeuroID

4x faster fraud detection

40% of manually approved fraud cases identified as risky by NeuroID

30% reduction in digital onboarding costs

Proactive protection against evolving attacks

CUSTOMER CHALLENGES

Unnecessary identity verification costs incurred by high fraud volume

Gaps in fraud detection allowing fraudulent applications to be manually approved

Unable to stay ahead of evolving fraud tactics as a large, popular attack target

A top 5 bank was struggling to stop third-party fraud in their large onboarding volume. The bank's size made them a popular attack target for fraudsters eager to unleash their newest and most advanced tools. Attacking fraudsters were able to work their way downstream in the bank's onboarding flow, prompting unnecessary data calls along the way. Some even made it past a manual review and successfully infiltrated the bank's ecosystem.

With fraud techniques evolving faster than ever, by the time the bank could respond to one type of attack, a new one was already trying to knock down the door. The bank needed a solution that could accurately detect sophisticated fraud early in the onboarding process and could also handle their large volume without sacrificing performance.

Enter NeuroID

Looking to stop fraudsters earlier and close gaps in their fraud detection processes, the top 5 bank turned to NeuroID, a part of Experian. By analyzing users' behavior, NeuroID was able to detect risky users — including bots, stolen and synthetic identities and fraud rings — as soon as they began interacting with the bank's application. With behavioral analytics, these risky users could be denied before incurring costly checks downstream or prompting a manual review.

This improved top-of-funnel fraud detection was crucial in optimizing the bank's fraud stack: NeuroID correctly identified over 90% of the bank's verified fraud cases (including 40% of cases that were being manually approved) as risky, **detecting fraudulent accounts 4x faster than the bank's prior solutions.** Earlier detection meant fraudsters couldn't progress through the bank's onboarding flow and trigger unnecessary identity checks, resulting in a 30% reduction in digital onboarding costs.

How NeuroID Protects Against Sophisticated Attacks

Solving the bank's existing fraud problems was one challenge, but protecting against future attack tactics was another. Months after they first added NeuroID to their onboarding flow, the bank experienced a large attack spearheaded by advanced, next-generation fraud bots. These bots were supercharged by Generative AI (GenAI) with human-like capabilities, able to circumvent the bank's existing bot detection tools.

A NeuroID investigation revealed the bot-led attack, and the bank implemented NeuroID's newest bot detection signal in response. **The NeuroID signal stopped the next-generation fraud bots in their tracks, identifying 20,000 hyper-sophisticated bots that weren't detected by any other vendor in the bank's fraud stack.**

With NeuroID, the top 5 bank is able to stay ahead of evolving attacks and focus on maintaining their status as an industry leader.

Past performance does not guarantee future results. Results may vary and this case study is not necessarily representative of all use of our products and services.

A top 5 bank struggled to stop sophisticated fraud attacks in their massive application volume. The bank was finding fraudsters after they made it through their onboarding flow, with some even being manually approved as legitimate customers.

With unnecessary identity verification costs compounding the bottom-line impact of fraud attacks, the bank looked to optimize their fraud stack. Their fraud team needed a solution that could stop fraudsters faster.

The bank implemented NeuroID at the top of its onboarding funnel. NeuroID's top-of-funnel decisioning instantly optimized the bank's fraud stack, **accurately detecting fraud 4x faster than the bank's existing solutions** and preventing fraudsters from progressing to costly identity verification checks and manual reviews.

NeuroID continues to protect the bank against evolving fraud attacks, including a recent hyper-sophisticated bot attack that wasn't detected by any other vendor in the bank's fraud stack. With NeuroID protecting its onboarding flow, the bank can focus on serving its large customer base without worrying about lurking fraudsters.