Case study

Leading consumer financial merchant

How behavioral analytics helped a leading merchant close post-login fraud detection gaps.

Challenges

- Multiplatform ecosystem brought high traffic and frequent flow changes.
- Evolving account takeover schemes pressured existing login defenses.
- Organized fraud rings infiltrated customer accounts at scale. Existing tools could spot individual fraud cases, but couldn't connect them to reveal coordinated attacks.

Results

- Increased fraud detection by 2X
- 200+ integration points across the ecosystem

15% of previously approved sessions flagged as risky

Fraudsters expose gaps in high-traffic, high-risk environments

Evolving fraud threats, including bots, MFA bypass tools and organized fraud rings, placed customer accounts at risk. Limitations in existing tools prevented the merchant from fully understanding the coordinated attacks targeting them.

Under increasing pressure to prevent sophisticated account takeover (ATO) schemes, the merchant's fraud team sought to strengthen its existing fraud stack while maintaining a frictionless experience for legitimate users. They needed a solution that could adapt to frequent form and flow changes across its multiplatform environment, scale effectively with high-traffic volumes and deliver precise risk signals without introducing unnecessary friction.

Case study

Leading consumer financial merchant

The Experian solution

The merchant implemented NeuroID's Account Defense solution from Experian across its digital ecosystem in one of the most technically rigorous integrations taken on by Experian's behavioral analytics experts.

The rollout covered over 200 integration points, including login, password reset, marketplace and transaction flows. At each point, NeuroID delivered a frictionless, real-time analysis of behavior, device and network risk.

Compared to the merchant's previous fraud stack, NeuroID detected twice as much fraud in web sessions and significantly improved device recognition. Of the sessions the incumbent stack had labeled as "new" devices, NeuroID identified that 50% were in fact returning devices. By recognizing high-risk returning devices, NeuroID flagged an additional 15% of risky sessions the incumbent tools had previously approved.

Among those additionally identified risky sessions, NeuroID's fraud ring intelligence discovered many groups of accounts linked by shared device usage. One network included over 10,000 connected profiles, revealing organized fraud attacks that had previously gone undetected.

NeuroID's team helped the merchant blocklist these devices and stop the fraud ring's attack in its entirety rather than just one device at a time. This newfound visibility enabled the merchant to increase their auto decline and review rates without negatively impacting genuine returning users.

Now, the merchant relies on NeuroID to monitor activity across all interaction points on its platform. By delivering more accurate fraud detection and uncovering organized fraud rings, NeuroID helps the merchant reveal coordinated ATO attacks and stop them before they escalate.

Timeline

1. Looking to protect its cross-platform ecosystem from costly fraud across login, password reset, marketplace and transaction flows, the merchant's fraud team begins its search for a solution that can improve upon its existing fraud stack.
2. The merchant integrates NeuroID's Account Defense API at over 200 points, providing continuous session monitoring, real-time analysis of behavior, and device and network signals.
3. NeuroID detects twice as much high-risk traffic compared to the merchant's incumbent tools and uncovers organized fraud rings, including one with 10,000+ profiles.
4. Insights enable threshold adjustments, reducing manual reviews without adding friction for legitimate users.

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 855 339 3990
experian.com