

How a global money transfer leader reduced annual ATO-driven losses by \$900k

Challenges

- Account takeover attacks carrying an average loss of \$300 per incident
- Daily fraud stack adjustments kept pace with evolving fraudsters, but required continuous attention
- Fast-paced transactions required frictionless fraud detection

Results

- 56x lift in chargeback predictive power
- 2% Increase in conversion rates

\$1.4 Million
in annualized savings

Challenges

This provider runs one of the most sophisticated fraud prevention ecosystems in the industry. They are supported by a highly skilled team and a dynamic rules engine with thousands of rules and daily adjustments designed to keep pace with evolving new fraud tactics. Their stack already included leading device and network intelligence tools, and they continuously refined models to stay ahead of evolving threats.

But in a landscape where fraud tactics evolve daily, even the strongest defenses benefit from incremental gains. The provider sought performance optimization, improved predictive power, fewer false positives and reduced operational overhead, without adding friction for legitimate customers.

Each successful account takeover carried an average \$300 loss, plus additional costs tied to false positives and manual reviews. The challenge was about strengthening an already advanced stack to make it more cost-efficient and scalable. They needed a solution that could seamlessly integrate, deliver measurable improvements and support their digital-first ambitions without slowing innovation.

The Experian Solution

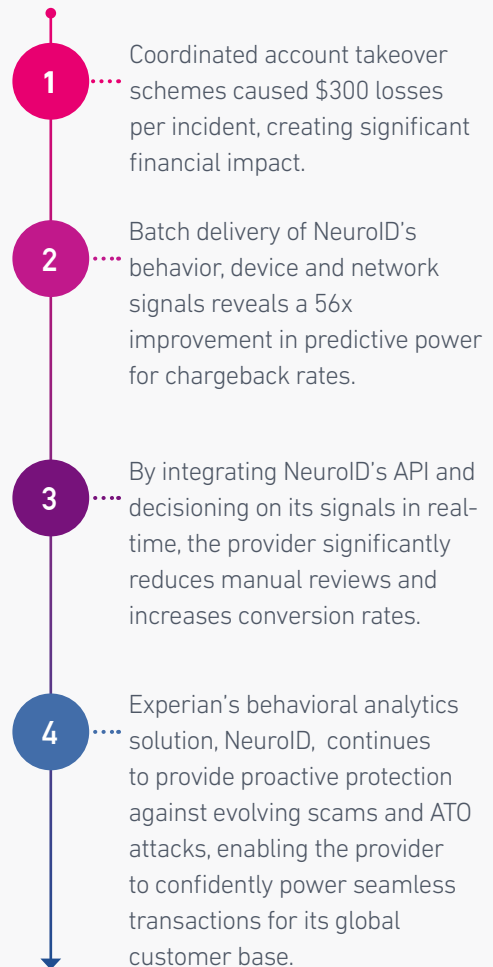
Experian's NeuroID Account Defense introduced a new layer of intelligence to the provider's already advanced fraud stack. The engagement began with batch delivery of behavioral, device, and network signals, giving the fraud team visibility into high-risk profiles and enabling proactive intervention. Early results were compelling — high-risk users identified by NeuroID had a 6% chargeback rate, a 56x lift in predictive power compared to baseline. This insight validated the provider's decision to add NeuroID as an incremental performance enhancer rather than a replacement for existing tools.

Building on this success, the provider integrated NeuroID's API for real-time decisioning at the transaction stage. High-risk users were either blocked or subjected to additional verification, while low-risk returning users enjoyed a frictionless transaction experience. This shift stopped fraudulent transactions while also improving customer experience, driving a 2% increase in conversion rates and reducing manual reviews for high-risk transactions.

Today, NeuroID is a core component of the provider's fraud stack, assessing risk during and after login and powering real-time decisioning at transaction. These capabilities have meaningfully cut fraud-related costs. The provider achieved \$850,000 in savings from incremental fraud capture alone. Total annualized gross savings reached \$1.4 million, driven by reduced fraud losses, chargeback fees, manual review costs, and optimization of other fraud tools.

The provider relies on NeuroID to proactively protect customers' accounts from evolving ATO schemes. NeuroID's link analysis uncovers fraud rings that had previously gone undetected, while behavioral signals provide early warning signs of bot attacks and scams. NeuroID empowers the provider to shut down threats before they escalate — stopping fraud, improving customer trust and ensuring secure scalability for future growth.

Timeline



experian® | NeuroID