neuroID

Payment Processor Pinpoints Thousands of Fraudsters & Saves Millions with NeuroID

$10M of potential annual fraud loss savings

100,000+ dormant fraudsters identified

Real-time decisioning on behavioral data before account opening

Scalable fraud mitigation without added friction to customer onboarding

CUSTOMER CHALLENGES

3M+ customers served and high-growth goals

Increase in bad actors making it past onboarding

Manual reviews **too costly and inefficient**

Goal: To optimize onboarding for genuine customers and decrease fraud without adding friction.

A prominent payment processor servicing about 3 million commercial U.S. customers needed to optimize a seamless onboarding process for genuine customers that was also efficient for early fraud detection. While using a two-step process to mitigate fraud risk at the onboarding and transaction stage, they still saw a high volume of bad actors bypass the onboarding check—leading to an uptick in dormant fraud accounts. With these fraud mitigation strategies falling short, the payment processor turned to custom solutions and manual reviews, which proved too costly.

They knew their key challenge was to combat fraud effectively without hurting operational efficiency. So, they chose NeuroID.

Enter NeuroID

Looking to find fraud sooner, the payment processor selected 6 months of previously observed user behavior data to evaluate a new use case. NeuroID picked out confirmed fraudsters nearly 90% of the time by the users' data entry patterns alone. By providing this level of top-of-funnel confidence, NeuroID could have provided the payment processor with $10M of annual fraud loss savings from chargebacks, manual reviews, investigation, deactivation, and downstream data calls costs associated with declining future fraudsters.*

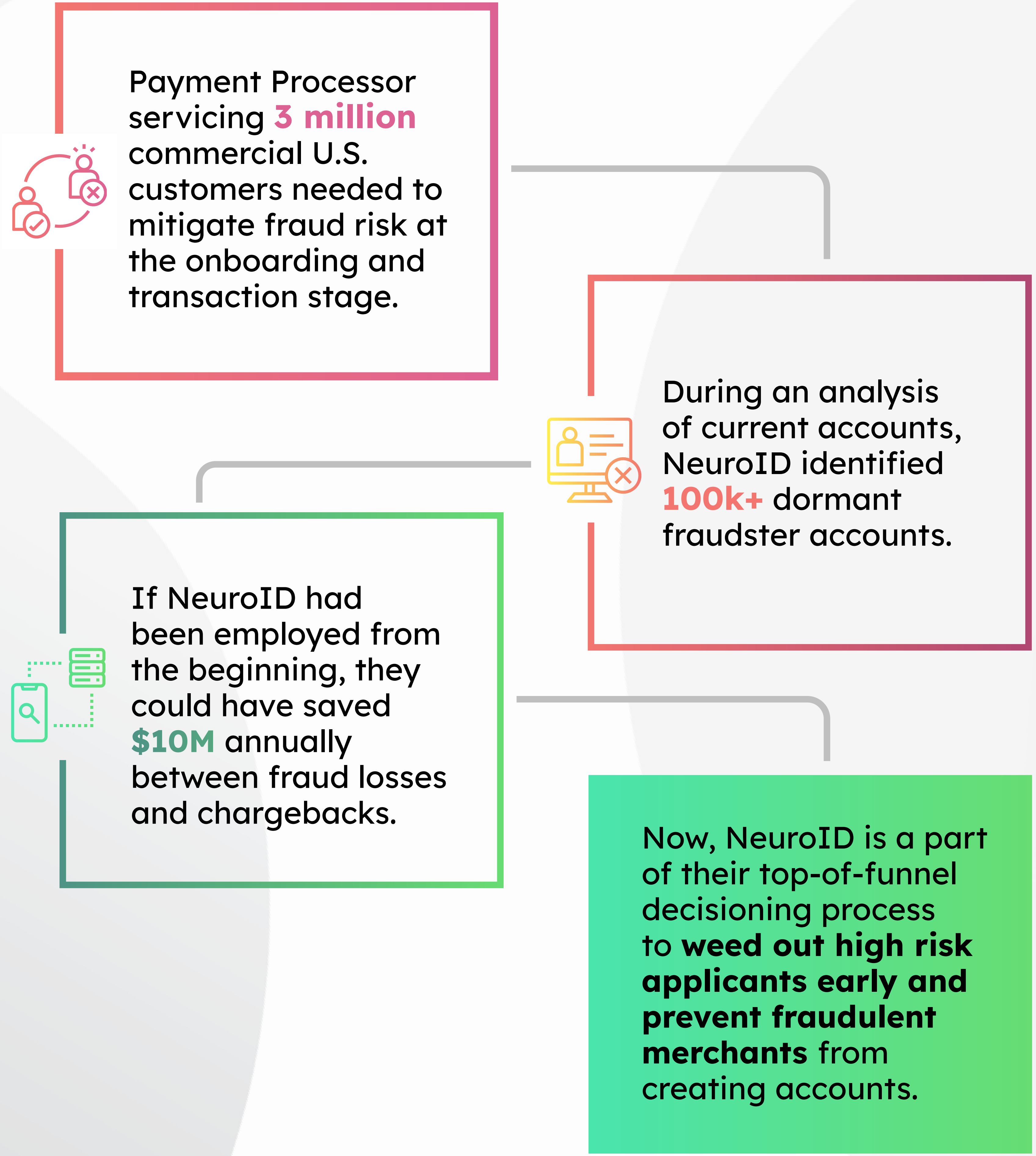
*False Positive Ratio: 0.003:1 (FPs:TPs)

Further analysis found 100,000+ dormant fraudsters—active accounts tied to hundreds of fraud clusters connected through browser IDs. These fraud clusters ranged from 5 to 60 accounts connected to the same browser. NeuroID caught the thousands of dormant fraudsters not just through their matching browser IDs, but also by analyzing all of the users' demonstrated high risky behavior, such as making in-page copy edits on first name and last name.

Impact of NeuroID

NeuroID analyzes consumer behavior using machine learning to accurately detect consumer segments that exhibit fraudulent characteristics indicative of fraud rings, automated bots or scripting activity, identity theft, synthetic identity usage, and other third-party fraud patterns. Now in place as part of the payment processor's account onboarding fraud mitigation, NeuroID assesses their user's intent in real time for sub-second decisioning on approve, deny, or review. This approach helps reduce the pressure on the payment processor's fraud stack and manual review teams by discretely weeding out fraudsters.

If NeuroID had been employed from the beginning, the payment processor could have saved an estimated $2.2M in fraud losses and $7.8M in fraud chargeback costs per year.



Payment Processor servicing **3 million** commercial U.S. customers needed to mitigate fraud risk at the onboarding and transaction stage.

During an analysis of current accounts, NeuroID identified **100k+** dormant fraudster accounts.

If NeuroID had been employed from the beginning, they could have saved **$10M** annually between fraud losses and chargebacks.

Now, NeuroID is a part of their top-of-funnel decisioning process to **weed out high risk applicants early and prevent fraudulent merchants** from creating accounts.