When Fraud Rings Attack:

CREDIT CARD ISSUING FINTECH

How monitoring digital behavior at scale **prevented more than $800k in fraud losses** for a high-growth credit card issuing fintech company.

early detection | sophisticated attack | $800k saved | 60k+ fraud attempts

The Client

In Q3 2021, a credit card issuing, hyper-growth fintech was celebrating hitting their highest customer growth rate, ever.

The Attack

A sophisticated fraud ring caught wind of the issuer's success and attacked, with the goal of using a coordinated effort to overwhelm the system.

The Impact

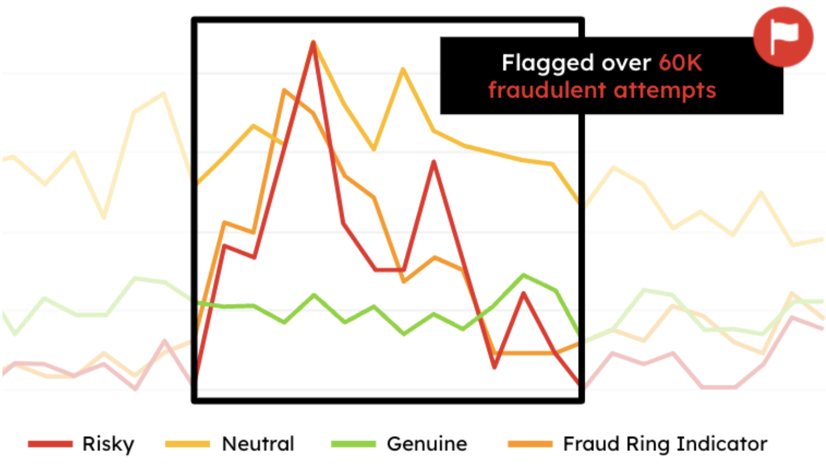
The issuer's fraud team started pending—and then outright declining—all applicants from a particular acquisition channel.

False declines were potentially costing the issuer hundreds of thousands of dollars. But they couldn't afford to trust anyone while knowing such a highly aggressive attack was in progress.

The NeuroID Solution

NeuroID's behavior-based identity solutions identified behavior directly related to the fraud ring. NeuroID alerted the credit-card issuer to each fraudulent applicant. Most of these bad actors would have been missed otherwise.

Digital Intent Over Time



The Result

NeuroID saved the issuer more than $800k in fraud loss and caught fraud that the issuer's existing fraud and risk tools had missed.

ID Crowd Alert™

- ☑ Alerted to sharp increase of fraudulent behavior around PII, indicating low familiarity
- ☑ Identified abnormal spike in risky applicant volume
- ☑ Identified fraud missed by issuer's existing stack
- ☑ **Prevented $800K in losses**

Learn more at **neuro-id.com**

Case studies describe our past work on real cases, but are not intended to guarantee that current or future customers will achieve the same results.

> "NeuroID is a necessity."
>
> - Manager, Fraud and Risk, Credit-Card Issuing Fintech