

EARLY PRESCREENING.

How ID Orchestrator’s real-time behavioral analytics prevented \$3 million in annual losses for a publicly traded unsecured lender.



early detection

fraud defense

>\$3M saved

applicant segmentation

The Client

A large, publicly traded fintech lender wanted to expand its existing fraud tools to defend against more complex fraud schemes.

The Attack

Sophisticated fraud rings noticed the fintech’s growing business and focused their attacks. By augmenting their traditional fraud solutions with behavior, which included device-based risk assessments, the lender prevented over \$3 million dollars in annual losses.

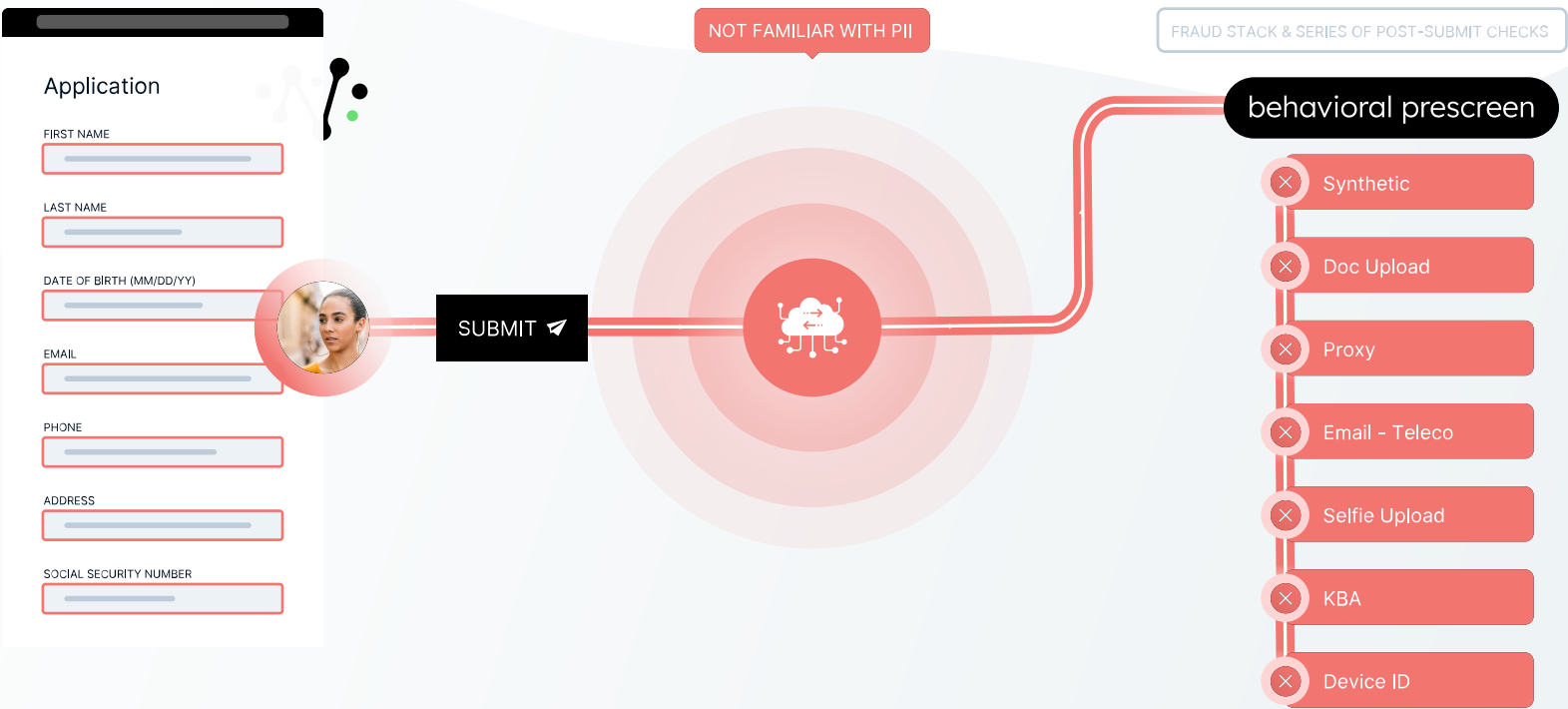
The Impact

NeuroID’s behavioral signals triggered prescreening rules for fraudulent applicants, without affecting the account opening experience for genuine customers. This prevented loan funding for 1,500 fraudulent applications, worth on average \$2,200 each. These fraudsters were otherwise missed by existing tools.

Furthermore, NeuroID saved the lender an estimated additional \$1 million in fraudulent loan applications that originated through the lender’s secondary loan platform.

ID Orchestrator

ID Orchestrator from NeuroID provides real-time intent flags that identify applicants with elevated risk. **NeuroID saved the lender more than \$3 million in fraud losses** and caught fraud that the lender’s existing fraud and risk tools had missed, including device-based risk solutions. By understanding the nuances of behavior, the lender added an additional layer of security without adding any friction to the account opening process.



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

VISIT
NEURO-ID.COM

[learn more](#)

- Assigned risky flags via API to each fraudulent applicant without using, storing, or collecting any PII
- Identified fraud missed by lender’s existing stack
- Prevented more than \$3M in fraud losses