Case Study

Identified Incremental Testing pattern across multiple Merchants with robust monitoring.

Background & Challenges

Monitoring team identified a complex card-not- present (CNP) fraud scheme affecting multiple online merchants. While initial transactions appeared authentic, advanced behavioral analytics uncovered a systematic probing attack designed to escalate transaction values gradually. This method exploited vulnerabilities within the payment authorization process, increasing financial risk and highlighting sophisticated fraud tactics that bypass conventional detection measures.

Fraud Scenario Overview

Phase 1

Initial Testing at Merchant A

- A cardholder initiated several low-value transactions (e.g.,
- $2.99), all of which were approved using valid credentials (CVV, ZIP, etc.).
- Transaction amounts gradually increased within a short timeframe.
- The sequence ended when a high-value transaction was declined, indicating the system's upper limit had been discovered.
- This highlighted a classic "threshold testing" technique, where fraudsters evaluate how much risk or monetary value can pass before a block occurs.

Phase 2

Strategy Shift to Merchant B

- After the high-value decline at the first merchant, the same card details were utilized on another e-commerce platform with no prior history.
- The low-value transaction sequence restarted and was once again approved.
- This pivot confirmed intentional adaptation—upon hitting the threshold at one merchant, the fraudster immediately resumed testing at another, seeking to evade existing risk controls.

Phase 3

Key Observations

- Same device/browser ID observed across both platforms, with only minor proxy variation (same ASN, geolocation).
- Identical card data (number, expiry, CVV, ZIP) used in both locations.
- Attack was executed within minutes, indicating coordinated and automated behavior.
- The pattern reflected an ongoing, adaptive learning approach—fraudster continually tweaked their tactics after encountering system countermeasures.

Key Results

50%+ Faster Fraud Detection - AI and behavioral analytics improved response times, minimizing financial damage.

30%+ Reduction in Fraud-Related Losses – Enhanced detection accuracy and real-time monitoring reduced fraudulent transactions.

Saurabh Bharti
Vice President, Analytics and AI

Let's Connect

Sukruth Pillarisetti
Senior Vice President, Analytics & AI

About Straive

As a data analytics and AI operationalization company, we don't just build top-tier data analytics and AI solutions—we integrate them seamlessly into your core workflows. This approach drives enhanced efficiency, improves user experience, and boosts revenue, setting you apart from the competition.

Serving a diverse range of industries— including Pharmaceutical & Life Sciences, Logistics, Supply Chain & Manufacturing, Research & Publishing, Information Services, EdTech, Banking & Financial services, and Retail Tech, Entertainment & Media— we have a global client base spanning over 30 countries.

Our strategically positioned resource pool operates across seven countries, including the Philippines, India, the United States, Nicaragua, Vietnam, the United Kingdom, and Singapore, where the company is headquartered.

www.straive.com contact@straive.com