Straive

Case Study

Preventing Online Shopping Fraud though in-depth investigation: Safeguarding Cardholders Against Fraudulent Merchants

Background & Challenges

A large financial institution detected a surge in fraudulent e-commerce transactions involving low-value amounts across multiple customer accounts. Fraudsters exploited vulnerabilities by executing high-frequency, identical transactions EX:($9.99) through suspicious merchants and IP addresses, suggesting automated scripted fraud. These transactions originated from risky IP locations and were concentrated on specific dates — 07/18/2025 and 07/20/2025 — across card.

The fraud scheme affected multiple customers and involved fake or compromised merchants, resulting in unauthorized charges and increased risk of card compromise.

Objectives

Deploy operational and monitoring controls to proactively identify and prevent e-commerce fraud through the following actions:

- Reduce Financial Losses: Flag and stop unauthorized low-value transactions to protect customers and minimize monetary impact.
- Enhance Fraud Detection: Identify rules and indicators to catch transaction patterns involving identical amounts and rapid succession across cards.
- Preventing Merchant Abuse: Identify and block suspicious merchants abusing platforms for fraudulent activities.
- Improve Response Time: Ensure quick action on flagged cards and transactions to stop fraud at early stages.
- Strengthen Monitoring: Leverage IP tracking, time-based velocity checks, and MCC codes to detect and prevent repeat offenses.

Approach to Combat Online Shopping Fraud

Advanced Rule-Based Detection System

- Flagged txn's with identical amounts EX:($9.99) across multiple cards.
- Detected high-frequency activity from the same or similar merchants.
- Monitored specific risk patterns involving MCC 5816 (Digital Goods).
- Highlighted automated/script activity based on transaction timestamps and IP origin.

Velocity & IP-Based Monitoring

- Enabled tracking of transaction frequency per card and IP address.
- Correlated activity to specific risky geolocations (e.g., VPNs, unusual countries).
- Analyzed patterns on specific high-risk dates to uncover coordinated fraud efforts.

Merchant Blocking & Compliance Rules

- Identified and blocked fraudulent merchants (example):
- *Aura Artistry Inc.
- *CanineHappy.com
- *UniqueComf.com
- Implemented rule under MCC 5816 to prevent further fraudulent merchant activity.
- Shared findings with relevant compliance and risk teams for regulatory alignment.

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.

Straive

www.straive.com
contact@straive.com