Graph-Powered Fraud Detection in Payments Ecosystem

Challenge

A large e-commerce firm faced a rise in coordinated fraud involving: Fake merchants and customers placing orders to trigger payouts.
Reused device IDs, IP addresses, and payment instruments across multiple accounts. Rule-based systems detecting only individual anomalies, missing ring-level collusion. Transaction-level data lacked relational visibility between entities.

Objectives

To identify and prevent collusive fraud rings in real-time by leveraging graph network connections and relationship-based anomaly detection, enhancing fraud prevention accuracy while reducing false positives.

Approach

➤ Built a multi-entity payment network graph connecting: Customers, payment instruments, merchants, devices, IPs, and delivery partners.
➤ Defined edges (relationships) such as "used same card," "shared IP," or "delivered from same address."

Solution

➤ Created a graph database with nodes (entities) and edges (relationships) for the transactions.
➤ Computed network centrality, degree, betweenness, and clustering coefficient for every entity
➤ Implemented Breadth-First Search (BFS) to explore connections up to two hops away.
➤ Built unsupervised clustering models on graph metrics to detect abnormal clusters of linked accounts
➤ Provided risk dashboards highlighting fraud rings and top suspicious clusters.
➤ Integrated real-time alerts into the transaction authorization engine.

Key Results

27% Fraud loss reduced within three months

$3.5 M Saved annually

About Straive

Straive

www.straive.com   contact@straive.com