Fraud Detection and Prevention Analytics

The Challenge

Cyber fraud costs organizations billions of dollars each year. The financial impact of fraud, waste and abuse (FWA) has been climbing rapidly in large part due to the increased number of adversaries online and expanding access to resources globally. Enterprise teams dealing with fraud are overwhelmed with the mountain of data to analyze, to find the needle in a haystack of needles. Analytics tools utilizing machine learning, with ability to prioritize incident analysis based on risk, is essential to effectively manage the burgeoning cyber security challenges in today's environment.

The Solution - Data Analytics for Fraud Detection and Prevention

First-generation data models have been used in the past for identifying fraud abuse. This technique, however, only looks at historical data and statistical models to predict fraud in a community or area. Machine learning and advanced data analytics provide a state-of-the-art method to analyze large volumes of data and predict anomalous behavior that can help prevent large scale frauds. In addition, data analytics facilitate risk scoring of individual users, consumers or entities and detect meaningful information on potentially risky users and real-time analysis of user behavior.

Types of Cyber Fraud

Cyber fraud falls into the categories and criminal abuse scenarios found below.

Financial Fraud

- **Money Laundering** - These cases include money being transferred between suspicious entities in smaller deposits of money, used to allay suspicion of money laundering and to evade anti-money laundering reporting requirements.
- **Merchant Fraud** - Abuse cases include merchants performing payment reversals inappropriately, as well as other methods of cyber manipulation of financial transactions and credit card fraud.

Healthcare Claim Fraud

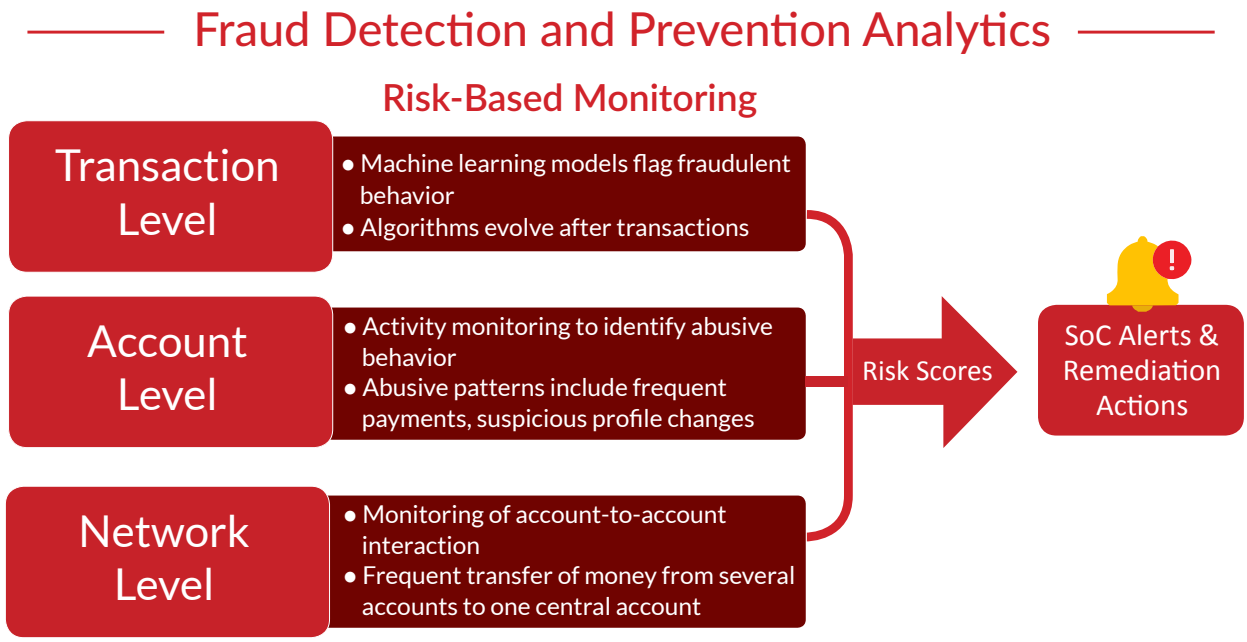
- **Provider Fraud** - Provider fraud represents approximately 90% of healthcare fraud, where fraudulent practices are designed to obtain illegitimate profits for the provider by using methods such as billing for services not provided, billing for a non-covered service as a covered service, falsifying service data, unnecessary drug prescriptions, and more.
- **Consumer Fraud** - Methods utilized to commit consumer fraud include medical identity theft, falsifying claims from non-existent clinics, organized crime against insurance companies, etc.

E-Commerce and Retail Fraud

- **E-Commerce and Retail Fraud** - These cases include fraud at point of sale or within enterprise environments. For example, a customer service representative accessing data of important customers for personal gain, without a business reason, such as an incoming support call or case. These must be detected and alerted in real-time to prevent abuse.

How GRA Can Help

The Gurucul Risk Analytics (GRA) platform provides a holistic risk-based approach for fraud detection of both internal and external users, using award-winning machine learning algorithms and an open big data architecture. Gurucul data science architecture creates a unique risk score for each internal user, customer or provider entity, using context-driven sensors from public and private data and transactions. Gurucul's open big data platform ingests both structured and unstructured data and aggregates risk context for intelligent predictive fraud detection.



Solution Feature Highlights

Financial Fraud Analytics

Analytics for merchant fraud, money laundering, and credit card hacking. Use cases include cyber fraud detection and deterrence, as well as for treasury, accounting, payments, and areas concerning funds transactions. Anti-money Laundering (AML) use cases include payment misreporting and unusual commodity trading or transactions.

Linking Data from Multiple Sources

GRA can link data from a multitude of sources to provide a contextual view, and highlight anomalous transactions, based on historic user and community profiles. The GRA system can analyze public records, mine and normalize data, and risk score fraud and abuse.

Healthcare Claims Fraud Analytics

GRA links data from a multitude of sources to provide a composite view of a patient's condition, and highlight anomalous transactions, based on historic user and enterprise profiles, and public records. GRA analyzes and risk scores fraud and abuse, which covers provider fraud, including billing irregularities and falsifying serviced data, as well as, consumer fraud, with detecting medical identity theft, false claims, and more.

E-Commerce & Retail Fraud Analytics

Challenges covered by these fraud analytics involve point of sale fraud, or within enterprise environments, which address external users in physical retail environments. These cases also include internal users accessing data of important customers for personal gain. As well, these analytics manage the overwhelming onslaught of heightened online transaction cycles, such as Cyber Monday, and other seasonal commercial events.

Real-Time Transactional Surveillance

GRA uses real-time and near real-time ingestion for transactional surveillance and can identify potential fraudulent transactions on the fly. This provides timely identification and risk-based status of both provider and fraud cases.

Fraud Detection and Prevention Analytics – Business Value

- **Comprehensive, real-time fraud monitoring** - Using big data, Gurucul provides a true 360-degree view of transactional activity for both enterprise physical locations, as well as, online transactional activity, facilitating rapid response and remediation of potential fraud activity.
- **Robust and flexible search capabilities** - With contextual search, using big data to mine linked users, accounts, structured and unstructured data, real-time risk scoring capabilities are delivered at the transaction, account and network levels, for holistic fraud analytics.
- **Rapid remedial response, ensuring reliable security** - Empowered by the most advanced, award-winning machine learning algorithms, GRA delivers the capability to detect and predict fraud incidents, and to empower rapid SoC incident responses, to ensure critical fraud prevention with dynamic efficiencies.
- **Prioritized security monitoring, with low false positives** - For both physical enterprise environments, as well as online cloud transactions, GRA addresses consumers, users and entities with self-learning and self-training machine learning algorithms, constantly drawing meaningful context from big data, to assure the highest caliber of risk-based and real-time fraud analytics results.
- **Reliable revenue protection, strengthening the bottom line** - Rather than struggling with a constant stream of unknown threats, GRA Fraud Detection and Prediction Analytics allows an enterprise to concentrate on its prime objectives for products and services offerings, and to dedicate key resources on the initiatives that promote expanding revenue streams and growth in the marketplace.

Awards

About Gurucul

Gurucul is changing the way enterprises protect themselves against insider threats, account compromise, and data exfiltration on-premises and in the cloud. The company's user and entity behavior analytics (UEBA) and identity analytics (IdA) technologies use machine learning and predictive anomaly detection algorithms to reduce the attack surface for accounts, unnecessary access rights and privileges, and identify, predict and prevent breaches. Gurucul technology is used globally by large enterprises in finance, banking, insurance, manufacturing, hi-tech, pharmaceutical and retail.

GURUCUL | 222 N. SEPULVEDA BLVD., SUITE 1322, EL SEGUNDO, CA 90245 | 213.259.8472 | INFO@GURUCUL.COM | WWW.GURUCUL.COM