VALOORES

Enterprise Fraud Management (EFM) and Geospatial Impact for Retailers

Enterprise Fraud Management (EFM) is a critical component for retailers and organizations in safeguarding against various forms of fraud. One key aspect of EFM is Transaction Monitoring, an internal management practice crucial for overseeing accounting, vendor relationships, purchases, and deals. This document explores the significance of Transaction Monitoring within EFM, emphasizing its role in accounting, vendor management, purchases, and deals. Additionally, it delves into the Geospatial Impact on EFM, elucidating how it can be employed to monitor the behaviors of employees, vendors, and customers, including creating link analysis.

To successfully navigate through this fraud pandemic era, retailers ought to reexamine how to determine who is reliable and who is not.
Success will require core capabilities, this is where VCIS takes the lead.

Table of contents

Introduction

Enterprise fraud management (EFM) supports the detection, analytics and management of fraud across users, accounts, products, processes and channels. It monitors and analyzes user activity and behavior at the application level, and watches what transpires inside and across accounts, using any channel available to a user. It also analyzes behavior among related users, accounts or other entities, looking for organized criminal activity, fraud rings, corruption or misuse.

Transaction Monitoring is an integral aspect of EFM, crucial for maintaining internal controls and preventing fraudulent activities across various organizational domains. The integration of geospatial technology enhances EFM capabilities by providing a spatial context to transaction data, enabling effective behavior monitoring, link analysis, risk management, and the adoption of a risk-based approach. By leveraging both Transaction Monitoring and geospatial insights, retailers and organizations can fortify their defenses against fraud and ensure the integrity of their financial processes.

Companies are moving towards digitisation, meanwhile, cybercriminals are mastering the art of exploiting businesses to fulfill their illicit intents. 2022 witnessed a 50% surge in money laundering fines. Worrisome statistics make the transaction monitoring process a new normal within the retail sector.

Enterprise fraud has undergone major changes in the last years, and recent trends have made fraud management a top priority for retail businesses.

As cases of fraud have grown, those institutions have sought ways to streamline their fraud responses while expanding their capabilities. This is where the concept of enterprise fraud management becomes important.

Enterprise fraud management is when an organization’s fraud processes and platforms are united in one place, in a coherent way, to enable real customer centricity and create efficiencies across the whole business to fight fraud.

Enterprise fraud management, or EFM, is a holistic approach that encompasses fraud detection, prevention and responses across all customers, products, and channels.

Transaction Monitoring in EFM

Know Your Transaction (KYT) means to proactively and reactively identify payments and business arrangements and flag suspicious transactions for manual review.
Transaction monitoring is a required practice for firms that move money on behalf of clients and businesses. It helps firms in preventing money laundering, terrorist financing, and other crimes that challenge safety across the globe.

VALOORES Transaction Monitoring is a complete solution that lets businesses streamline their due diligence processes. Detecting suspicious activity by screening against international watchlists, many Data sources and verifying identities in less than a second, is a wholesome technology to keep you ahead of cybercriminals.

Accounting

Transaction Monitoring in accounting involves scrutinizing financial transactions to detect anomalies, irregularities, or signs of fraudulent activity. This includes monitoring financial statements, expense reports, and payroll transactions.

Vendors

In vendor management, Transaction Monitoring ensures that vendor transactions align with established agreements. Any deviations or suspicious activities are flagged for further investigation, mitigating the risk of fraudulent vendor practices.

Purchases

Monitoring transactions related to purchases involves scrutinizing payment processes, ensuring compliance with procurement policies, and identifying any irregularities in purchasing patterns that could indicate fraudulent activities.

Deals

Transaction Monitoring for deals focuses on scrutinizing financial transactions associated with business deals, mergers, acquisitions, or partnerships. This helps in preventing financial fraud and ensuring transparency in business transactions.

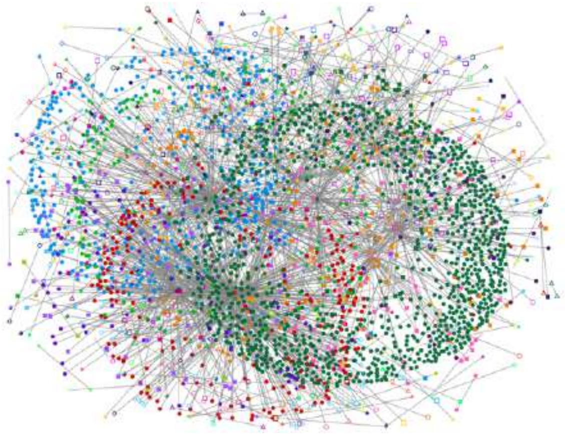
Geospatial Impact on EFM

Monitoring Behaviors

Geospatial technology plays a pivotal role in monitoring the geolocation of employees, vendors, and customers. This enables the tracking of their physical movements and activities in real-time, contributing to the detection of suspicious behavior.

Link Analysis

By integrating geospatial data with transaction records, link analysis can be performed to establish connections between individuals, entities, and locations. This aids in identifying unusual associations or patterns that may indicate fraudulent activities.



Prevention Methods

Utilizing geospatial data, organizations can implement proactive prevention methods. For example, if a specific region has a history of fraudulent activities, enhanced security measures or targeted employee training can be implemented to deter potential fraud.

Risk-Based Approach

The Risk-Based Approach in Enterprise Fraud Management (EFM) involves tailoring strategies and resource allocation according to the identified risks within an organization. Geospatial data plays a pivotal role in enhancing this approach by providing a contextual understanding of risks associated with specific locations.

Contextual Understanding of Risks

Geospatial data incorporates the spatial dimension into risk assessment. By associating risk factors with specific geographical areas, organizations gain a nuanced understanding of the unique challenges and vulnerabilities present in different locations. For instance, certain regions may exhibit higher instances of fraudulent activities due to historical patterns, socioeconomic factors, or other contextual elements.

Resource Allocation

With a geospatially informed risk-based approach, organizations can allocate resources more strategically. Rather than adopting a one-size-fits-all strategy, they can tailor their efforts based on the level of risk identified in different geographical areas. This involves concentrating resources, such as personnel, technology, and monitoring tools, in locations with higher perceived risks.

Proactive Risk Mitigation

Geospatial insights enable organizations to be proactive in mitigating risks. By identifying high-risk areas in advance, they can implement targeted measures to deter fraudulent activities. For example, heightened security protocols, increased monitoring, or specific training programs for employees in regions with elevated risk can be deployed.

Dynamic Risk Management

Geospatial data adds a dynamic element to risk management. It allows organizations to adapt their strategies based on real-time changes in the risk landscape. This adaptability is crucial in an environment where risks may evolve over time, and new patterns may emerge, necessitating a flexible and responsive risk management approach as well as identifying high-risk geographical areas or patterns of fraudulent behavior in specific locations.

- <u>Uncover fraud patterns</u>

Device fingerprinting and AI help you identify suspicious patterns so you can stop fraud rings before they can harm your business.

- <u>Onboard users without friction</u>

The real-time data enrichment module automatically spots obvious fraudsters while letting good customers in with no added friction to the user journey.

- <u>Build better risk rules</u>

Detect suspicious devices with VCIS robust default rule set or create custom rules that tackle threats unique to your business.

Improved Decision-Making

By integrating geospatial data into risk assessment, decision-makers have a more comprehensive and informed basis for making strategic choices. They can weigh the geographical context of risks alongside other relevant factors, leading to more effective and contextually aware decision-making.

Enhanced Overall EFM Effectiveness

Incorporating geospatial data into the risk-based approach contributes to the overall effectiveness of EFM. It allows organizations to focus their efforts where they are most needed, optimizing resource utilization, and creating a more resilient and adaptive fraud prevention strategy.

In summary, the integration of geospatial data into the Risk-Based Approach in EFM empowers organizations to understand and manage risks in a location-specific context. This not only improves the efficiency of resource allocation but also enables a proactive and dynamic approach to fraud prevention, ultimately enhancing the overall effectiveness of the EFM strategy.

Real-Time Analysis and Results

When it comes to enterprise fraud prevention, there are two crucial factors: how much data you can work with, and how efficiently you can analyze it. Which is to say, real-time analysis is a must. This is particularly important in the context of KYC checks, where you don't want to keep your users waiting too long. Data enrichment should also be performed in real-time, even when it's to build an alternative credit score using your users' digital footprint.

How to Prevent & Detect Enterprise Fraud

Thanks to data analysis and interpretation, detecting fraud has never been easier yet fraudsters will continue to innovate so having an EFM system that focuses on the key areas of abuse your industry faces is important. Depending on what's required, your business can look at either working with a complete end-to-end EFM system or create a more tailored multi-layered approach built up of differing products. Some of the most important features to include in any EFM system are:

- Team Roles and Responsibilities
- Real-time Transaction Monitoring
- Machine Learning
- Behavioral Analytics
- Decision Making
- Access to Alternative Data
- Fraud Risk Assessment / Scoring
- Reporting Procedures
- Investigation Process
- Multi-factor Authentication

Data harnessing and advanced analytics

Using centralized data repositories to store customer accounts, customers behaviors, and transaction data from multiple channels and production systems as well as external sources. Organizations are already using high-performance computing technologies to analyze massive portions of data in real time and create detailed customer profiles. This makes for organized data that can be used for investigation of money laundering and fraud as well as for surveillance purposes.

Cloud-based detection and authentication

Fraud detection platforms are increasingly becoming cloud based. Cloud deployments bring the advantages of automatic upgrades, flexibility, reduced capital expenses, and scale capabilities as per demand. While executives may be hesitant to send customer information to the public cloud, instances of cloud platforms with security measures superior to on-premise systems show that the benefits can outweigh the concerns.

Predictive fraud models

Rule-based fraud identification can be improved by combining sophisticated predictive fraud models and analysis of massive data sets. To make models more accurate and improve fraud detection, analytic techniques such as pattern analysis to identify anomalous behavior and link analysis to scrutinize hidden frauds are being used.

Enterprise case management

By leveraging enterprise case management, banks are making investigation workflows more efficient. Retailers and Businesses are also battling fraud by using data visualization tools for faster decision making and robotic automation for optimal business processes.

Next-generation authentication mechanisms

Businesses need to verify customer identities while delivering on high expectations seamlessly. Techniques such as voice and speech recognition and desktop analytics are helping organizations prevent fraud. While outsourcing customer service, partnering with experienced vendors that have innovative, secure authentication tools and processes in place can drive process efficiency and time savings while ensuring customer experience is not affected.
Introducing next-generation enterprise fraud solutions will deliver diverse benefits, including reduced total cost of ownership, improved staff productivity,

visibility into fraud exposure, as well as assist companies in protecting brand reputation.

Since fraudsters will always find new ways to commit fraud, companies need future-ready fraud prevention solutions as part of their financial crime compliance program. Some key capabilities of such solutions will include functional ease, technological superiority, and market potential. Banks also need to ensure adequate internal supervisory procedures and systems to regulate fraud, without hindering customer experience.

Payment network

Graph database and ML algorithms can be used to represent, store, and analyze the relationships within customers and other financial actors, not connected exclusively through payments, but possibly based on other personal information (e.g. similar address locations, phone number, similar IP etc). This solution allows fraud specialists to explore the network to study criminal patterns, fraud rings, money-laundering schemes, and allows data scientists to incorporate new information into transaction monitoring models (e.g. measures of proximity between sender and payee), leading to advantages across fraud prevention/ detection, errors identification and response.

Geospatial-based transaction monitoring

Geospatial information, propagated by phone apps, ATMs or POS devices, could provide evidence of where the customer is located with respect to past transactions, providing further evidence whether or not they are acting legitimately.

Once geolocated, historical transactions are collected and aggregated, safe zones can be generated by clustering of geo-data points for each customer. While a customer is operating from these areas, their fraud risk can be mitigated and (if no other threats are detected) payments could be allowed to proceed frictionlessly.

Deep fraud pattern data mining

Advanced analytics and data mining can drill-down on huge volumes of transactions. It can identify correlation patterns and hidden fraud schemes in data, as well as designing feedback-loop cycles that reprocess historical payments as soon as new information is available.

All this information is of critical importance and can be visualized on BI dashboards for supporting operations and decision-making to improve the end-to-end fraud management process.

Intelligent automation process of fraud operations

Most manual work by fraud analysts consists of repetitive tasks, such as monitoring, often similar, incoming alerts and reporting. Implementing RPA and intelligent process automation can ease this effort and allow specialists to focus on value-add tasks. Full control of the anti-fraud system is always guaranteed, and automation can be scaled according to transaction workloads.

Business Intelligence-powered fraud investigation

Business domain expertise is not really challenged by data-driven transformation. On the contrary, human contribution is augmented using BI techniques and real-time dashboards. These help and accelerate fraud analysts in their investigation, while enabling complex analysis and visualization of geospatial or graph data.

ABOUT VALOORES
Careers
Press Release
Quotes

CONTACT US
Access Dashboards
Office Locations
E-mail

LINES OF BUSINESS
in'Banking
in'Technology
in'Insurance
in'Healthcare
in'Government
in'Analytics
in'Academy
in'Retail
in'Multimedia
Webinars

SERVICES
in'AML
in'Regulatory
in'Merch
in'IRFP
In'AI/BI
in'KYC
in'Fraud Management
in'Via
in'Consultancy
in'Profit
in'Campaign
in'IFRS9