Multilayered Fraud Detection with Cyber Intelligence

Posted on May 29, 2024

For centuries, fraudsters have devised cunning schemes to steal from unsuspecting victims. Though fraud methods have evolved, their impact remains devastating. In 2023 alone, victims worldwide lost more than US$1 trillion to fraud.

The latest INTERPOL assessment of financial fraud reveals that technology significantly enables cybercriminal groups to launch large-scale and sophisticated campaigns. This trend calls for a similar technology-empowered cybersecurity approach. Organizations need to respond in kind and utilize modern technology to detect and prevent fraud.

Companies are already dedicating a significant portion of their resources to combating fraud, with estimates suggesting as much as 6–11% of annual revenue is spent on prevention efforts.

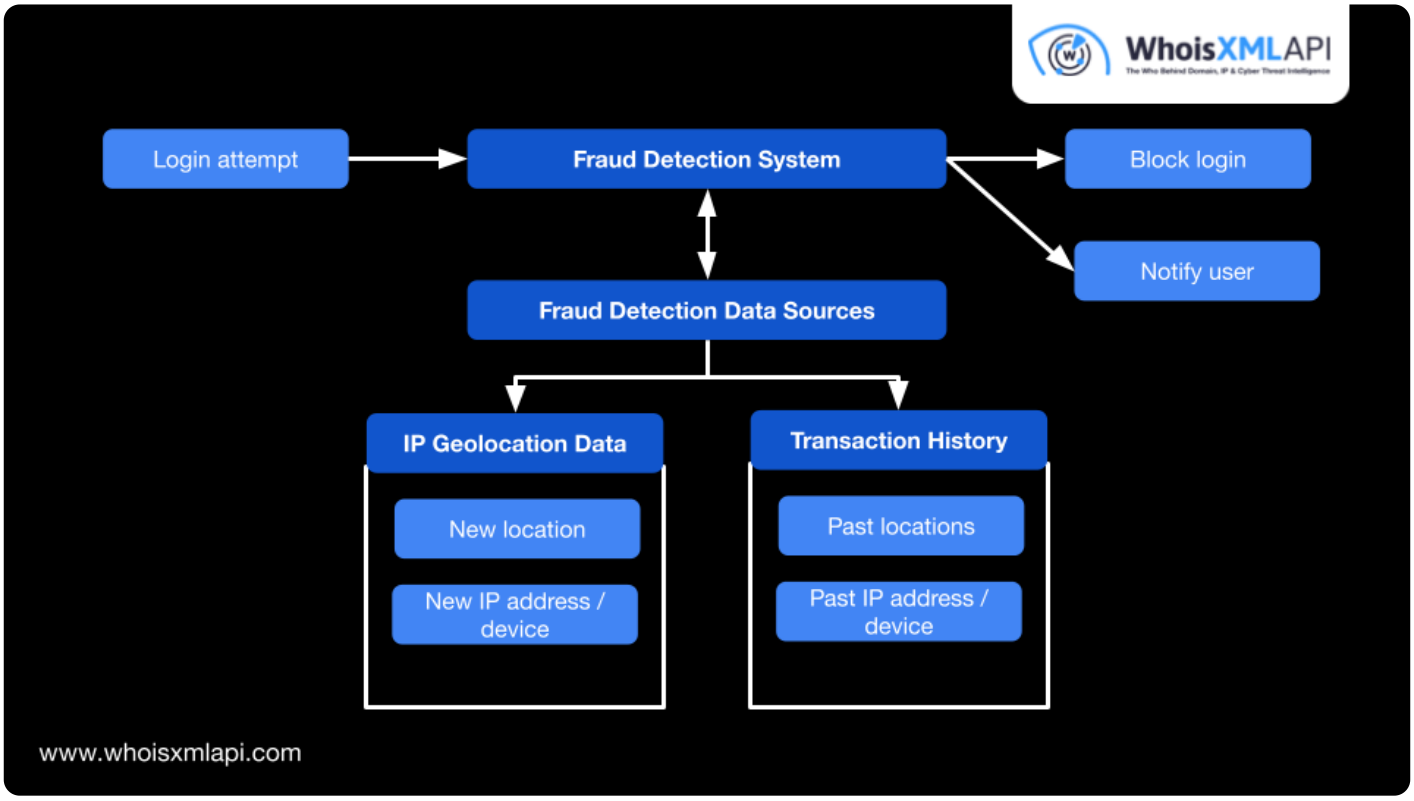
However, not all fraud detection and prevention solutions and methods are created equal. Effectively tackling this ever-evolving threat requires leveraging modern techniques and high-quality data to stay a step ahead of fraudsters.

How Does Fraud Detection Work?

Fraud detection is a multilayered approach that combines technology usage, data analysis, and human expertise to identify and prevent fraudulent activities. It typically begins with data collection and aggregation from various sources, including transaction records, user behavior data, and external sources, such as open-source intelligence (OSINT). Combined with DNS, IP, and domain intelligence, these data sources can enable fraud detection systems to gain Internet-wide context, detect impersonation, and employ predictive analytics.

Once the data is gathered, fraud detection systems are engineered to identify anomalies and

unusual patterns that deviate from typical user behaviors. For example, a login attempt from a new location or device may be considered suspicious. The system would be triggered to block the attempt and notify the user through previously verified communication channels.



The process may sound straightforward, but its effectiveness relies heavily on high-quality and up-to-date data to avoid false positives and accurately flag fraudulent activities and entities. Too many false positives, where legitimate transactions are flagged as suspicious, can prompt businesses to abandon anti-fraud solutions.

Know Who You're Talking to with Internet-Wide Context

Knowing who you're talking to (KWYTT) intelligence is a critical first line of defense for organizations across all sectors, given the sheer number of digital identities organizations may communicate with every day—suppliers, vendors, resellers, distributors, customers, users, and

other parties.

KWYTT is an extension of the Know-Your-Customer (KYC) policy that financial institutions are required to comply with. It supports the zero-trust approach to network security, espousing continuous identification and verification of all entities.

Supplementing user transaction and behavior data and other key fraud detection intelligence sources with reliable and accurate DNS, IP, and domain data can help fraud detection systems provide much-needed context, notably to banks. In particular, Internet-wide context can enhance critical KYC and KWYTT processes, such as:

- **Identity access management (IAM):** When assessing the overall risk of a login attempt, IAM and fraud detection systems may glean insights from IP geolocation data. If a user logs in from an unexpected location using a different ISP or an IP address associated with malicious activity, the system can trigger additional authentication steps, flag the attempt for review, or temporarily block user access.

- **Account creation and onboarding:** Many fraudsters utilize temporary or disposable email addresses that are difficult to trace. Fraud detection during onboarding involves ensuring new customers sign up with their real identities. Integrating email verification services into systems can identify disposable email addresses, prompting further scrutiny. In addition, analyzing an IP address during account creation can help companies pinpoint a user's location. This location can trigger a higher risk score if it coincides with a known cybercrime hotspot. Getting flagged, however, doesn't automatically translate to fraud, but it can initiate additional verification steps.

- **Transaction verification:** Checking for transaction red flags may include analyzing fund origins and destinations, along with other risk factors like transaction amounts, historical spending habits, and beneficiary information. Transactions originating from or directed to offshore accounts or unexpected regions, particularly those with higher concentrations of financial crime, may warrant further investigation, especially when the sender or recipient is new.

- **Third-party risk management (TPRM):** Fraudsters may create fake company profiles and target organizations with a history of working with a specific type of supplier or exploit a

recent announcement about a new supplier partnership. Therefore, verifying a supplier's legitimacy through multiple channels is essential before entering into business with them. That may involve contacting them through the phone numbers listed on their websites instead of via email. This step can be supplemented with passive due diligence, such as checking the supplier's domain ownership details, IP geolocation, and website category and reputation data.

Impersonation Detection

Fraudsters often masquerade as trusted entities like banks, credit card companies, or even friends and colleagues. In fact, the Federal Trade Commission (FTC) received more than 330,000 reports of business impersonation scams and around 160,000 reports of government impersonation scams in 2023.

Microsoft, Google, LinkedIn, and Apple are among the most impersonated brands in Q1 2024, and a significant part of the impersonation can be detected using DNS traces. The table below illustrates this detection, showing proportionate samples of the number of domains registered in Q1 2024 containing the names of the three most-impersonated brands and the number of malicious domains using the same brand names.

Most-Impersonated Brands	Sampled Number of Domains Containing the Brand Names Registered in Q1 2024	Sampled Number of Malicious Domains Containing the Brand Names
Microsoft	972	1,766
Google	3,869	1,383
LinkedIn	535	133

Sources: *Reverse WHOIS and Threat Intelligence API*

Predictive Analysis

Predictive analytics is a powerful technique that focuses on early intervention by identifying potential fraud instances before attacks can occur. The approach typically uses machine learning (ML), deep learning, and other modern artificial intelligence (AI) techniques to analyze historical data and current trends. This technique has proven effective, with companies reporting up to an 80% fraud detection rate with an 89% accuracy.

Predictive analytics is used by predictive threat intelligence sources that feed fraud detection systems with cyber resources that threat actors can potentially use. For example, the Early Warning Phishing Feed detects newly registered domains (NRDs) that resemble those belonging to popular brands and text strings commonly used in impersonation campaigns. Meanwhile, the Early Domain Generation Algorithm (DGA) Detection Feed detects groups of suspicious DGA-created domains commonly used in malware-enabled attacks.

Using predictive threat intelligence can enable fraud detection systems to flag suspicious resources for further scrutiny before allowing them to communicate with protected applications.

Conclusion

The global fraud detection and prevention market is projected to grow from US$43.97 billion in 2023 to US$255.39 billion by 2032. These systems can be further classified based on application (e.g., insurance claims, money laundering, and electronic payments), solution (e.g., fraud analytics, governance, and authentication), enterprise type (i.e., small, medium-sized, or large enterprises), deployment (i.e., on-premises or cloud-based), and industry (e.g., healthcare, financial, telecom, and transportation).

However, regardless of type, the effectiveness of a fraud detection system would depend greatly on the quality of data it uses.

Take your fraud detection capabilities to the next level with Internet-wide and predictive cyber intelligence. Contact us now for more information about our data solutions.