

Fraud Ring Gallery

A Strategic Guide to Fighting Fraud Rings
with Real-World Examples



Contents

An Overview of Fraud Ring Dynamics 01

Real-World Fraud Ring Examples 02

 Check Fraud in a Regional Bank

 ATO and Fake Accounts in a Leading E-commerce

 Financial Institution’s Fight Against a Coordinated Credit Card Scam

 A Multi-Stage Card Stacking Attack Hit a Prominent Payment Processor

How DataVisor Can Help You Fight Fraud Rings 10



An Overview of Fraud Ring Dynamics

Fraud rings represent a sophisticated and coordinated effort to commit financial or data theft on a scale far beyond individual fraudulent activities. Unlike isolated incidents of fraud, which might involve a single actor or a few transactions, fraud rings are characterized by their organized nature, often involving multiple individuals working together.

The defining feature of these rings is their scale, which not only amplifies the potential financial losses but also poses a significant threat to the reputation of the targeted organizations. Organized groups meticulously plan and execute large-scale attacks, leveraging new techniques that often elude traditional reactive rule-based and machine learning systems and exploiting those vulnerabilities to withdraw funds, steal identities, or engage in other illicit activities.



The landscape of fraud ring attacks has unveiled alarming trends and statistics that underscore the escalating challenge these groups pose. A notable fraud ring from Southeast Asia has executed one of the largest attacks on U.S. e-commerce platforms to date, illicitly acquiring goods valued at an estimated \$660 million. Furthermore, the resurgence of check fraud, alongside the proliferation of online access to Personally Identifiable Information (PII) has also played a pivotal role in enabling the growth of these large-scale, coordinated fraud schemes.

Fraud rings can specialize in various types of attacks, including but not limited to identity theft, check fraud, credit card skimming, phishing schemes, and loan fraud. Each type presents unique challenges and requires specific countermeasures.

As we delve deeper into the world of fraud rings, it's essential to recognize the complexity and diversity of these schemes. The following section will showcase real world examples of fraud rings that have been identified and disrupted, providing insight into the application of fraud detection and prevention strategies. By examining these examples, organizations can better prepare themselves to combat the ever-evolving threat of fraud rings, safeguarding their assets and maintaining the trust of their customers.



Check Fraud in a Regional Bank

Fraud Ring Overview

A group of fraudsters targeted a specific regional bank, exploiting its lax check deposit policy intended for customer convenience. They stole checks from mail, particularly targeting residential neighborhoods with street-side mailboxes. This policy inadvertently made the bank a prime target for the sophisticated fraud ring, resulting in a financial exposure.

Method of Operation

The fraudsters targeted homes during the first and last weeks of the month, coinciding with common check mailing times. Stolen checks were altered to change the payee and sometimes the amount. The scheme was executed by a well-coordinated network that recruited individuals as "mules" to deposit these checks into the bank accounts. Following deposit, funds were quickly withdrawn and sent to specific accounts, exploiting the time gap before the bank could realize it was fraud.

Highlights



Fraud Ring Pattern



Geographic Area

Many of the mail thefts originated from certain neighborhoods, marked by specific zip codes.



Unusual Behavioral

Quick deposits and withdrawals of the altered checks were a common pattern.



Mobile Deposits

A key pattern observed was the exclusive use of mobile deposit for all the altered checks, exploiting a vulnerability commonly found in many banks' mobile banking services.



Limited Transaction History

The accounts into which the checks were deposited, and from which funds were later sent out, often had minimal to no prior transaction history.



Similar Beneficiaries

Money was frequently transferred to a few similar beneficiaries, indicating unusual account linkages.



ATO and Fake Accounts in a Leading E-commerce

Fraud Ring Overview

A leading e-commerce company faced a critical challenge. A well-orchestrated fraud ring infiltrated their platform, reaching 100,000 accounts at its peak and posing a potential loss of millions of dollars.

Method of Operation

The fraudsters employed a two-pronged approach. Initially, they focused on Account Takeover (ATO) Fraud, utilizing data from the dark web to access and exploit dormant user accounts. This first phase involved small-scale fraudulent transactions to test the waters. However, the situation escalated rapidly with the second phase: mass registration of fake accounts. In an unprecedented move, the fraudsters created +15,000 fake user accounts within a few hours, using these to facilitate larger-scale financial fraud. Their methods constantly evolved, shifting tactics to avoid detection, and employing a mix of stolen and fake identities for their activities.

Highlights



Fraud Ring Pattern



IP and Device ID

It started with tracing similar IP addresses and device IDs used in fraudulent activities, providing an initial understanding of the operation's scope.



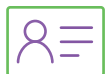
VPN and Data Centers

As accounts were shut down, the fraudsters frequently changed IP and device IDs. Many of the IPs were flagged as they predominantly originated from VPN services and data center addresses.



Payment Instruments

A deeper insight emerged from analyzing the payment instruments used in transactions. The consistent use of specific payment instruments across various transactions illuminated the fraud network.



Payout Account

A significant amount of funds from the seller accounts was funneled into a relatively small number of bank accounts which were associated with neobanks with lower KYC standards. Flagging those bank account numbers was the critical factor in unveiling the last link of the fraud chain.



Financial Institution's Fight Against a Coordinated Credit Card Scam

Fraud Ring Overview

A financial institution successfully exposed a sophisticated fraud ring by closely examining the similarities present in a series of credit card applications. Through meticulous analysis, patterns emerged that indicated a coordinated effort to deceive the financial institution.

Method of Operation

A social media influencer was orchestrating a series of webinars where participants are instructed on deceptive practices aimed at securing credit lines from specific financial institutions. The influencer provides guidance on how to falsify crucial information, such as income details and other personal data, with the explicit purpose of deceiving these financial institutions. It's worth to note that the webinar attendees, following the influencer's advice, had purchased emails from the dark web, and therefore, their addresses weren't flagged by third party signals.

Highlights



Fraud Ring Pattern



Webinar Referral Links

Applications were linked by referral URLs from webinars conducted by a social media influencer.



Similar Income

80% of applications declared that their monthly income is \$6,833.



Employer

100% of the fraudulent applications were listed as "self-employed".



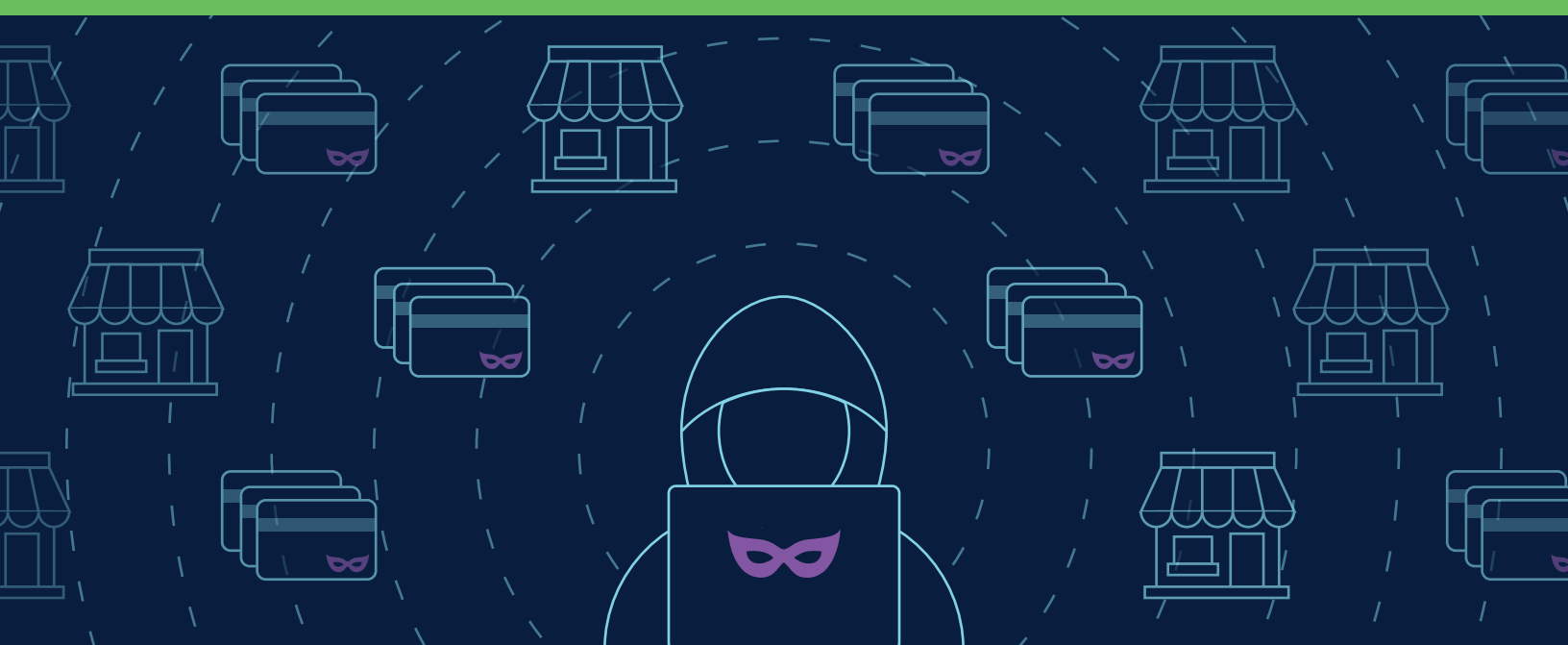
Unusual Application Times

A significant number of applications were submitted during odd hours, particularly in the middle of the night, flagging them as suspicious.



Consistent Email Domain

Applications frequently used the @outlook.com domain.



A Multi-Stage Card Stacking Attack Hit a Prominent Payment Processor

Fraud Ring Overview

In this case involving a major payment processor, a sophisticated operation involved numerous bad actors targeting various merchants to conduct fraudulent transactions. Their approach showcased a deep understanding of payment systems and a capacity to quickly adjust strategies in response to evolving security measures.

Method of Operation

The fraudsters implemented a multi-stage operation that began with a testing phase and rapidly escalated in complexity and scale. The initial phase involved targeting one merchant using this as a proving ground for their card stacking bot attacks. A card stacking bot attack is a method where automated software, or bots, rapidly test a large number of credit card numbers to identify which ones are valid and active.

As the operation progressed, the fraudsters quickly expanded their activities to include 10-15 different merchants each day. This expansion was not random; it was a calculated move to diversify their targets and reduce the risk of detection.

To facilitate this expansive operation, the fraudsters relied on the dark web to acquire the thousands of credit card details necessary for their scheme.

Highlights



Fraud Ring Pattern



New Merchants

After successfully exploiting a merchant a few times, the payment processor's models would begin to flag the fraudulent activity, prompting the fraudsters to move on to other merchants.



Card Transaction History

The cards used in the fraud were inactive for months prior to the attack. In addition, those cards never transacted in those countries or with those merchants before.



Repetitive Credit Card Bin

This repetition served as an initial indicator of fraud, as some of those bins were already flagged as high risk. However, due to the high false positive rate, this alone was not sufficient for conclusive fraud detection, necessitating the use of additional data points for a more accurate identification.



Digital Patterns

To maintain simplicity and speed in their operations, the fraudsters used consistent patterns across transactions. The detection models, however, began to identify these patterns, including consistent use of specific IP addresses, device IDs, email domains, and prefix patterns, along with transaction timestamps and amounts.

How DataVisor Can Help You Fight Fraud Rings

Combating fraud rings requires sophisticated detection capabilities and the ability to connect disparate pieces of information to uncover and understand the structure and operation of these fraudulent networks.

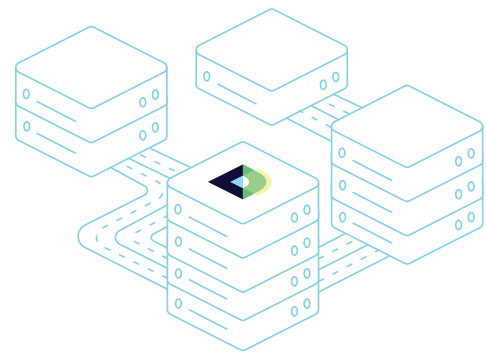
At DataVisor, we recognize the complexity of this challenge and offer a suite of products specifically designed to empower organizations in their fight against fraud rings. In this section, we will break down the necessary steps to combat fraud rings, highlighting key products within our platform that are crucial for this endeavor.

Creating a Centralized Intelligence Hub

At the core of any effective fraud detection solution lies the quality and robustness of data. High-quality, comprehensive data is the fuel that powers anti-fraud technology, making it essential for conducting effective fraud analytics.

Recognizing this, one of the foundational elements of our approach is the emphasis on acquiring a 360-degree view of customer activity. This comprehensive perspective is critical for creating a centralized intelligence platform that harnesses predictive power, providing actionable insights and enhancing decision-making processes.

DataVisor's **Data Orchestration** layer serves as the backbone of our fraud and risk management platform, seamlessly integrating diverse data sources into one single platform. By leveraging a flexible, data agnostic architecture, enabling real-time data transformation, and integrating third-party signals, organizations can effectively process and analyze data in real-time across the entire account lifecycle, across business units, and through various channels. Those capabilities create a unified view of customer behavior, significantly improving the detection and prevention of fraud rings.



Decoding Digital Identities with Device Intelligence

Understanding who's on the other side of a digital interaction is crucial, especially as fraudsters use advanced tactics like emulators and app cloners to disguise device IDs for large-scale attacks. Device intelligence is therefore essential for fraud teams, offering critical data to counteract these threats and uncover fraud ring patterns.

Our solution, **dEdge**, directly addresses these challenges. It's a comprehensive device intelligence platform combining device fingerprinting, risk assessment, behavior analytics, and edge computing. **dEdge** protects against digital threats by collecting over 100 device signals, generating unique device IDs, detecting sophisticated attack techniques, and analyzing behavior signals. This solution ensures organizations are equipped to identify and mitigate complex fraud schemes effectively, marking **dEdge** as an essential tool in modern digital security arsenals.



Transforming Data into Decisive Fraud Detection Indicators

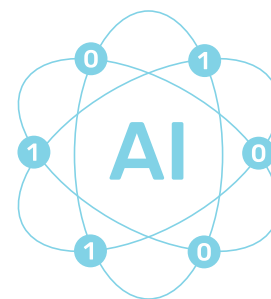
Following the consolidation of data in one single platform, the next critical step is making sense of this information. This is where feature engineering plays a vital role.

Feature engineering transforms raw data into crucial risk indicators that are pivotal for fraud detection. This transformation process includes the consolidation of various data sources into a standardized format, which is crucial for efficiently developing, testing, and deploying new fraud signals. The standardized features generated by this process are essential inputs for machine learning models and rule engines, facilitating rapid and automated decision-making processes. It's a critical step in uncovering patterns and relationships indicative of fraud rings.

Given the complexity and ever-evolving nature of fraud, **DataVisor Feature Platform** is designed with robust feature engineering capabilities at its core. These capabilities include supporting high queries per second (QPS) with low latency, conducting complex calculations of data attributes in real time, and the ability to swiftly create and test new features. Such features are vital for enhancing the detection abilities of models and rules, ensuring they are equipped to detect fraud rings effectively and in real time.



Unveiling Complex Fraud Schemes with Unsupervised Machine Learning

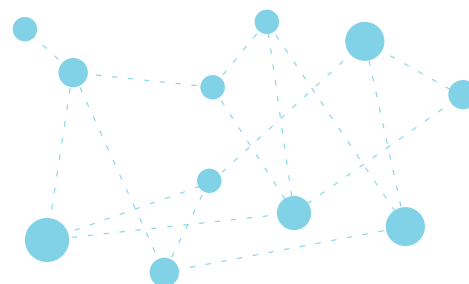


Following our discussions on the critical roles of data orchestration, device intelligence, and feature engineering, we arrive at a pivotal point: the identification of patterns and connections within the data. Possessing vast amounts of data is futile without the capacity to leverage it for detecting anomalies and predicting fraudulent behaviors.

Machine learning stands as a powerful ally in this arena, with its capability to learn from historical data (labeled data) and enhance predictions regarding fraudulent activities. Traditional models excel in identifying fraud perpetrated by individuals or recurring patterns of fraudulent activity. However, these models often fall short when confronting complex fraud schemes orchestrated by coordinated groups, or fraud rings, due to their reliance on previously identified patterns.

This gap is precisely where **DataVisor's Unsupervised Machine Learning (UML)** technology excels. Our **UML** approach does not depend on pre-existing knowledge of fraud patterns. Instead, it utilizes advanced correlation analysis and graph processing techniques to unearth the connections between fraudulent account behaviors. By creating clusters that reveal these linkages, our **UML** framework is uniquely equipped to detect and expose organized, mass-scale attacks.

Connecting the Dots for a Comprehensive View of the Entire Fraud Ring



To fully comprehend the scope of a fraud ring, it's essential to visually explore the connections stemming from fraudulent activities. While models and rules play a critical role in fraud detection, they might not capture every facet of a fraud ring. Hence, a link analysis tool becomes necessary to provide a complementary perspective on the data.

DataVisor Knowledge Graph, serves this purpose by enabling the visualization of customers and their connections based on shared entity relationships, such as IP addresses or emails, or transactional flows, like money movement. With **Knowledge Graph**, fraud teams can directly visualize and analyze data, identify various types of activities, and link multiple transactions to specific device IDs or IPs,

crucial for unveiling the complex web of fraud rings. It also enhances operational efficiency through its capability for bulk actioning, allowing teams to make decisions on numerous instances simultaneously, such as shutting down an entire fraud ring with one click.

Combining Knowledge Graph with UML significantly enhances fraud detection capabilities. While UML excels in clustering based on patterns identified by models, it might not capture all potential fraudulent connections, sometimes due to the risk of false positives or the unique value certain links provide that UML alone might overlook. This is where the Knowledge Graph proves invaluable. It allows for the exploration of connections that UML might not initially identify as significant, offering a comprehensive view of the entire fraud ring.

Summary

We've established that addressing fraud rings requires a comprehensive strategy, as these operations are complex and necessitate our highest level of diligence and strategic insight. Each component we've discussed - from data orchestration and device intelligence to feature engineering, unsupervised machine learning, and knowledge graph - serves an essential function in unveiling an entire fraud ring.



DataVisor's holistic approach empowers organizations to combat fraud rings more effectively, ensuring a fortified defense against evolving threats and maintaining the trust of their customers.

About DataVisor



DataVisor is the world's leading fraud and risk management platform that enables organizations to respond to fast-evolving fraud attacks and mitigate risks as they happen in real time. Its comprehensive solution suite combines patented machine learning technology with native device intelligence and a powerful decision engine to provide protection for the entire customer lifecycle across industries and use cases. DataVisor is recognized as an industry leader and has been adopted by many Fortune 500 companies across the globe.

