Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2022, 9(11):70-74

Research Article ISSN: 2394 - 658X

Fraud Types and Detection: Analysis

Khirod Chandra Panda[1]

[1]Asurion Insurance, USA
[1]khirodpanda4bank@gmail.com

ABSTRACT

Fraud is a pervasive threat that can have severe consequences for both individuals and businesses, often resulting in significant financial and emotional damage. Despite its prevalence, fraud can often go unnoticed until it causes harm, making robust fraud detection, management, and analysis measures crucial. Data from the Federal Trade Commission indicates a concerning trend, with reported fraud losses skyrocketing to $5.8 billion in 2021 and nearly doubling to almost $8.8 billion in 2022. California has been heavily impacted, recording an estimated $1,349 million in fraud losses in 2022.Given these alarming statistics, businesses and individuals must remain vigilant and proactive in combating fraud. Heightened awareness is essential, and understanding the various types of fraud, such as first-party, second-party, and third-party fraud, is crucial for implementing effective prevention strategies. First-party fraud involves individuals misrepresenting their identity for financial gain, presenting challenges in sectors like e-commerce where face-to-face interactions are limited. Second-party fraud occurs when individuals share their personal information for fraudulent activities, while third-party fraud involves using someone else's identity without permission. To combat these types of fraud, businesses can employ a range of strategies, including using multi-factor authentication, leveraging AI-based fraud detection tools, and educating users on recognizing and reporting fraudulent behaviors. Implementing a strong anti-fraud strategy is essential for safeguarding customer information, minimizing financial losses, and maintaining trust and satisfaction among stakeholders.

Key words: AML, Data, FRAML, Fraud, First party, Machine Learning, MFA, Second Party

---

INTRODUCTION

Fraud permeates various aspects of our lives, often unnoticed until it inflicts financial or emotional harm. Whether it's unauthorized credit card charges or identity theft, the repercussions of fraud can be severe. This underscores the critical importance of robust fraud detection, management, and analysis measures to safeguard individuals and businesses alike.

Data compiled by the Federal Trade Commission paints a sobering picture of the escalating threat posed by fraud. In 2021 alone, reported fraud losses surged by over 70%, amounting to a staggering $5.8 billion in consumer losses. By 2022, these losses soared to nearly $8.8 billion, with California bearing the brunt of the impact, registering an estimated $1,349 million in fraud losses.

These alarming statistics underscore the urgent need for businesses and individuals to remain vigilant and proactive in combating fraud. Heightened awareness is the first line of defense against fraudulent activities. Therefore, in this discussion, we will delve into the intricacies of fraud detection, management, and analysis. We'll explore how these processes function, their significance, and why they are indispensable for businesses.

Understanding the various types of fraud that businesses encounter is crucial for implementing effective prevention strategies. By dissecting the methods and motives behind fraudulent activities, organizations can deploy targeted countermeasures to mitigate risks and protect their assets. Through proactive measures and a comprehensive understanding of fraud prevention techniques, businesses can fortify themselves against the ever-evolving threat landscape, safeguarding their financial interests and reputation.

Fraud detection refers to the process of monitoring transactions and customer behavior to pinpoint and fight fraudulent activity. It is usually a central part of a firm’s loss prevention strategy and sometimes forms a part of its wider anti-money laundering (AML) compliance processes [1]. When fraud detection and its related

functions are integrated into a wider AML framework, the combination is sometimes referred to as fraud and anti-money laundering (FRAML) [2]. Regardless of the structure it belongs to, fraud detection relies on technological tools, subject-matter experts (especially analysts), policies, and procedures to function well.

LITERATURE REVIEW

Why is Fraud Detection important.

Quoting from a leading online analysis piece "Fraud detection is crucial for protecting businesses, consumers, and financial institutions from financial losses, reputational damage, and legal liabilities associated with fraudulent activities. It helps prevent fraudsters from exploiting vulnerabilities and safeguards assets and sensitive information." [3]

Fraud prevention and detection are crucial for several reasons. Firstly, they safeguard individuals and organizations against financial loss and damage to their reputation. Fraud can have a significant impact on a company's financial health and its relationships with customers, suppliers, and investors. Secondly, preventing and detecting fraud helps maintain trust and integrity within the business community by ensuring that transactions are conducted fairly and transparently. Additionally, effective fraud prevention and detection measures can help businesses maintain compliance with legal and regulatory requirements, which is essential for ethical and sustainable operations. Lastly, by identifying and addressing fraudulent activities, resources can be allocated more effectively, leading to improved operational efficiency and financial stability.

In traditional fraud prevention and detection approaches, firms aim to mitigate financial losses and uphold positive customer relationships. However, in certain jurisdictions, legislation mandates fraud programs for firms providing specific services, such as insurance providers in various US states. In the UK, the introduction of a "Failure to Prevent Fraud" offense in April 2023 holds firms accountable if they benefit from employee fraud without adequate fraud prevention measures. Additionally, on June 7, 2023, the UK's Payment Systems Regulator announced a new reimbursement requirement for firms whose customers fall victim to authorized push payment (APP) fraud.

Fraud detection is essential for companies to protect their customers' transactions and accounts by identifying fraud before or as it occurs. According to the FBI, in 2022, elder fraud victims in the US lost an average of $35,101 each, resulting in a total loss of over $3 billion. In 2021, global fraud losses exceeded $55 billion, facilitated by technology that enables illegal funds to cross international borders.

As awareness of the various types and complexities of fraud grows globally, firms should anticipate the introduction of more regulations and enforcement actions that will impact their compliance requirements. Even if a firm is not currently subject to direct requirements, fraud is a predicate offense for money laundering and may be linked to a broader pattern of criminal activity. By integrating fraud prevention into their overall risk management framework, firms can better protect consumers, ensure compliance, manage loss, and combat financial crime.

For businesses operating online, real-time fraud detection and prevention software are essential. Attacks come in many forms and affect businesses differently, but they are pervasive. According to PwC's 2022 Global Economic Crime and Fraud Survey (Fig 1), over half of organizations reported financial losses due to fraud, with a quarter experiencing losses exceeding $1 million. Additionally, fraud often disrupts business operations and lowers employee morale, with perpetrators increasingly including hackers and customers.

Fig 1. Fraud Trend

TYPES OF FRAUD

In general, fraud can be classified into three primary categories [4]: First-party fraud, Second-party fraud, and Third-party fraud. This classification is based on the perpetrator of the fraud and whose identity details were used or compromised. Understanding the various forms or types of fraud is crucial for devising effective strategies to combat financial crimes and fraudulent activities.

First Party Fraud

First-party fraud occurs when an individual intentionally misrepresents their identity or provides false information for financial or material gain. This deception can take various forms, such as inflating income, fabricating employment history, or misrepresenting financial circumstances to access services like loans, mortgages, or insurance policies. For instance, individuals might purchase expensive items on credit cards with no intention of paying, then deny making the transactions to claim chargebacks, leaving the retailer or merchant at a loss.

In the e-commerce realm, first-party fraud poses significant challenges as buyers and merchants rarely interact face-to-face, making it difficult to detect fraudulent activity. Merchants not only lose money but also the merchandise when fraudulent transactions occur. Various forms of first-party fraud include ghost funding, chargeback fraud, ACH fraud, lost in transit fraud, item not as ordered fraud, and mortgage application fraud.

First-party fraud is often mistakenly categorized as credit loss and written off as bad debt, complicating businesses' efforts to distinguish fraud losses from credit risk and make informed lending decisions. This type of fraud can be opportunistic, involving small-scale fraudsters acting individually or informally, or organized, orchestrated by criminal gangs or fraud rings. Some schemes, like sleeper or bust-out fraud, can be executed in both opportunistic and organized manners.

For instance, criminal organizations exploit the transient nature of university students' mobility, targeting them to purchase their identity credentials and bank accounts as they return to their home countries. Fraudsters often advertise in student unions or social media, luring cash-strapped students with offers of quick money. Similarly, individuals experiencing financial hardship due to unemployment may turn to fraud to cover expenses. With access to personal information and banking apps, criminals swiftly acquire credit fraudulently, using accounts for money laundering and other illicit activities. These crimes underscore the urgent need for improved fraud prevention measures to combat first-party fraud effectively.

Frist Party Fraud Prevention

Businesses can take proactive measures to defend against first-party fraud. Utilizing fraud prevention tools, for instance, enables them to blacklist individuals who have previously committed first-party fraud. This helps reduce the likelihood of repeat offenses.

Moreover, refining fraud detection software can assist in pinpointing the warning signs mentioned earlier, such as specific profile indicators. Identifying potentially suspicious customers allows the business to conduct further investigation and take appropriate actions, such as limiting account functionality for those associated with multiple addresses or users.

It's essential for businesses to recognize that fraud risks, including those related to first-party fraud, can evolve over time. Therefore, they should remain vigilant to new threats and scams, adjusting their strategies and responses accordingly. This ongoing vigilance is key to effectively combating fraud and protecting their operations and customers.

Second Party Fraud

Second-party fraud occurs when an individual knowingly shares their personal information or identity with another person or entity for fraudulent purposes. This type of fraud often involves the perpetrator using the shared information to carry out illicit activities without the knowledge or consent of the information provider.

One prevalent form of second-party fraud is money mulling, where an individual allows someone else to use their bank account to transfer funds in exchange for a fee. Despite appearing as a seemingly harmless act, money mulling can have serious consequences as the transferred funds may originate from criminal activities or money laundering, potentially financing terrorism, exploitation, or violent crime.

Detecting second-party fraud can be challenging compared to first-party fraud since it's difficult to determine whether the information provider willingly participated in the fraudulent activity. For example, an individual might share their personal information with a friend or family member who then uses it to make purchases from an unlinked device, making the transactions appear legitimate and complicating efforts to ascertain the individual's involvement.

Another instance of second-party fraud involves a fraudster persuading an individual to accept and transfer money from their account to another account, promising a share of the funds in return. Some individuals unwittingly fall victim to such schemes and become unwitting participants in money laundering activities.

Second-party fraud encompasses various forms, including money laundering and the creation of synthetic identities, where fraudsters use the shared personal information to fabricate new identities for further fraudulent activities. These fraudulent activities underscore the importance of robust fraud prevention measures and heightened awareness to combat second-party fraud effectively.

Second Party Fraud Prevention

To tackle second-party fraud [5] effectively within a business, professionals need to deploy strategies that match the speed and scale of financial criminals. Machine learning has emerged as the preferred technology for anti-money laundering (AML) teams to combat financial crimes on a large scale.

Help organizations to recognize suspicious behaviors.

Prioritize responses based on level of perceived risk.

Reduce manual intervention and false positives.

Help investigators remain compliant and assist law enforcement teams.

Third Party Fraud

Third-party fraud, also termed identity theft, happens when someone uses another person's personal data without permission for fraudulent activities. This stolen information, such as Personally Identifiable Information (PII), is used for unauthorized purchases or opening false accounts. Fraudsters might also fabricate new identities using stolen details, a practice known as synthetic identity fraud.

This type of fraud involves the perpetrator hiding their true identity behind that of another person or using a fabricated one. Third-party fraud is a common form of fraud where the victim is easily identifiable, making it simpler to detect within portfolios. Victims of third-party fraud may experience financial losses and damage to their reputation.

Globally, third-party fraud poses a significant issue, affecting individuals and businesses with various fraudulent schemes. Those involved in third-party fraud range from individuals trying to use stolen credit cards or take out loans in someone else's name to organized crime groups conducting large-scale fraud operations.

Although often involving the theft of personal details, third-party fraud can also include the use of synthetic identities created specifically for fraudulent purposes. The consequences of fraud reach beyond the direct victims, impacting financial institutions, retailers, and e-commerce stores targeted by fraudsters. Fraud incidents can lead to significant financial, emotional, and practical consequences, with many victims experiencing emotional distress after such incidents.

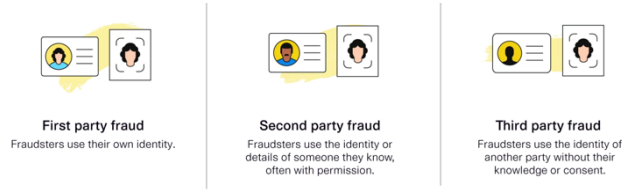

Fig. 2 Difference First, second, Third Party Fraud

Third-party Fraud Prevention

A strong anti-fraud policy is crucial for businesses to protect their reputation and build trust, which in turn helps safeguard customers from various threats. Here are some key aspects to consider:

Holistic approach: This involves integrating data from various sources, such as device IDs, customer behavior, and cross-channel transactions, to detect unauthorized purchases and payments.

- Improved customer experience: Analytic fraud models with self-learning capabilities adapt and enhance their accuracy over time, reducing false positives and ensuring a smoother experience for genuine customers.
- Deep behavioral networks: These networks learn optimal features directly from data, enabling rapid extraction of features that would otherwise take years to develop.
- Preventing identity fraud requires a joint effort from individuals and the companies they engage with. Basic practices like maintaining strong, unique passwords, using cybersecurity software, and being cautious on insecure networks are crucial. Educating users is also vital, as many third-party fraud incidents stem from human error. Increasing awareness about phishing emails and fake websites can significantly reduce fraudsters' opportunities.

Businesses must approach third-party fraud detection from both procedural and technical angles. While technology plays a crucial role, staff training and cyber awareness are equally important. To combat evolving fraud tactics, tech companies continually innovate with new fraud prevention solutions. These may involve machine learning, artificial intelligence (AI), or Open Source Intelligence (OSINT) [6] to automate additional checks on customer details.

Fraudsters are constantly seeking new ways to commit fraud, so vigilance and proactive measures are essential to stay ahead of them.

CONCLUSION

Having a strong anti-fraud strategy is essential for any organization that deals with online transactions and customer data. This strategy typically involves several key components:

Strong authentication: Implementing multi-factor authentication (MFA) can significantly enhance security by requiring users to provide multiple forms of verification before accessing their accounts.

AI and ML-based fraud detection tools: These tools can help identify fraudulent activities by analyzing patterns and anomalies in transaction data, enabling organizations to detect and respond to fraud in real-time.

User education: Educating users and customers on how to recognize and report fraudulent behaviors and activities can help prevent fraud before it occurs.

Encryption protocols: Using robust encryption protocols helps protect customer data from unauthorized access and data breaches, ensuring that sensitive information remains secure.

Implementing a comprehensive anti-fraud strategy is crucial for safeguarding customers' personal and transactional information, minimizing financial and reputational losses for organizations, and maintaining customer satisfaction and trust.

REFERENCES

[1]. ComplyAdvantage, "AML Compliance Program," ComplyAdvantage, Aug. 26, 2022. Online, Available: https://complyadvantage.com/insights/anti-money-laundering/aml-compliance-program/

[2]. S. Cameron, "FRAML: The convergence of fraud and money laundering," ComplyAdvantage, Feb. 13, 2021.Online Available: https://complyadvantage.com/insights/framl-fraud-and-money-laundering/

[3]. Fraudcom International, "What is fraud detection and why is it needed?" Fraud.com, Mar. 04, 2021.Online, Available: https://www.fraud.com/post/fraud-detection

[4]. E. Uk, "The different types of fraud and how they're changing," Experian UK, Nov. 29, 2020.Online, Available: https://www.experian.co.uk/blogs/latest-thinking/fraud-prevention/what-is-first-second-and-third-party-fraud

[5]. P. Evans and Featurespace, "A complete guide to second- and third-party fraud," Featurespace, Mar. 29, 2020. Online, Available: https://www.featurespace.com/newsroom/a-complete-guide-to-second-and-third-party-fraud/

[6]. "Top 10 OSINT (Open-Source Intelligence) Software & Tools | SEON," SEON, Nov. 28, 2021. Online, Available: https://seon.io/resources/comparisons/osint-software-tools/