ONLINE PAYMENT FRAUD DETECTION

PRESENTED BY

Pk prithishakaran

III YEAR ,KVCET,CSE

NM ID :autlecse202104

GMAIL ID:prithishakaran@gmail.com

Problem statement

Payment fraud poses a constantly evolving menace that carries significant consequences for businesses, financial institutions, and consumers alike. Notably, recent cyber perils like

The scope of these challenges extends beyond unauthorized transactions, encompassing identity theft, account takeovers, and even instances of “friendly fraud,”

What is Payment Fraud?

- Payment fraud is a complex and constantly changing form of deceitful or unlawful transactions that seek to gain financial benefits through unauthorized and deceptive activities. It encompasses a wide range of illicit actions, including unauthorized transactions across different payment channels such as credit cards, virtual checks, direct debits, and phone payments. Fraudsters frequently employ advanced methods to manipulate transaction data to appear legitimate, thus evading anti-fraud systems

Online Payment Fraud Detection

01

Online Payment Fraud Detection

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

02

Your Text Here

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

03

Your Text Here

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

04

Your Text Here

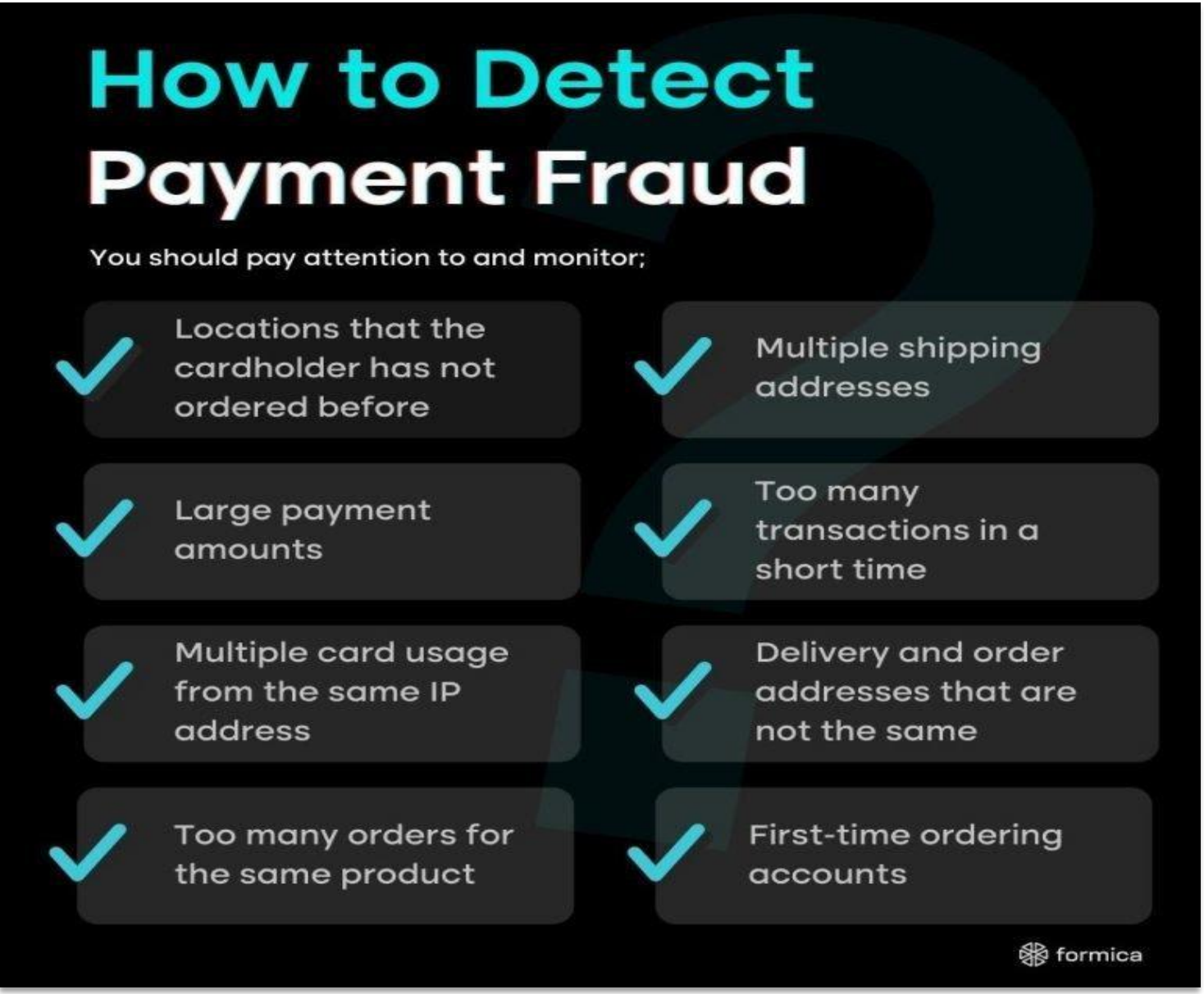
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

How Does Payment Fraud Happen?

- Identity Mimicking: The hackers use a Virtual Private Network (VPN) to effectively replicate the IP addresses originating from the customary locations where the pilfered credit cards are typically utilized.
-
- Device Fingerprinting Evasion: The hackers employ emulators to replicate the devices typically linked to the cardholders, to deceive and gain unauthorized access.
-
- Transaction Camouflaging: In order to minimize the risk of immediate detection, they initiate their activities by making inconspicuous transactions such as arranging airport transfers or reserving accommodations at budget hotels

Shifting Fraud Landscape

- The landscape of payment fraud is experiencing unprecedented growth and advancement, transforming into an intricate and sophisticated challenge. The digitization of banking and payment services, although providing convenience to customers, has introduced a paradoxical situation. It has unveiled an array of vulnerabilities that are eagerly exploited by fraudsters, thereby presenting a significant dilemma.
-
- The rapidity with which transactions are presently processed can be viewed as both advantageous and disadvantageous. While it undoubtedly improves the overall customer experience, it also limits the opportunity for comprehensive scrutiny, consequently creating a more favorable environment for fraudsters to exploit



Rising Scale and Complexity

Quick Transactions, Less Time for C

Sophistication of Fraud

Fragmented Resources

Types of Payment Fraud

- Account Takeover (ATO)
- Synthetic Identity
- Business Email Compromise
- Identity Theft
- Carding
- Chargeback Fraud
- Account Takeover (ATO
- Business Email Compromise
- Card-Not-Present (CNP) Fraud
- Account Enrollment Fraud

The Difference Between Payment Fraud and Friendly Fraud

- Perpetrator: Payment fraud typically involves a perpetrator who is often an external party seeking to deceive. Conversely, friendly fraud entails the customers themselves perpetrating the fraudulent activity.
- Intent: Payment fraud is a deliberate act carried out to deceive. Occasionally, there may be instances of friendly fraud resulting from misinterpretation, for instance, when a family member unknowingly purchases without the cardholder's knowledge.
- Merchant Relationship: Friendly Fraud refers to a regrettable breach within the merchant-customer relationship, where the customer, in essence, manipulates the merchant. In contrast, Payment Fraud does not entail such intricate relationship dynamics.
- Resolution: Friendly fraud can often be resolved through effective communication between the customer and the merchant, fostering a mutually beneficial resolution. Conversely, payment fraud typically necessitates the involvement of legal channels and may lead to the imposition of criminal charges.

3 Pillars of Payment Fraud

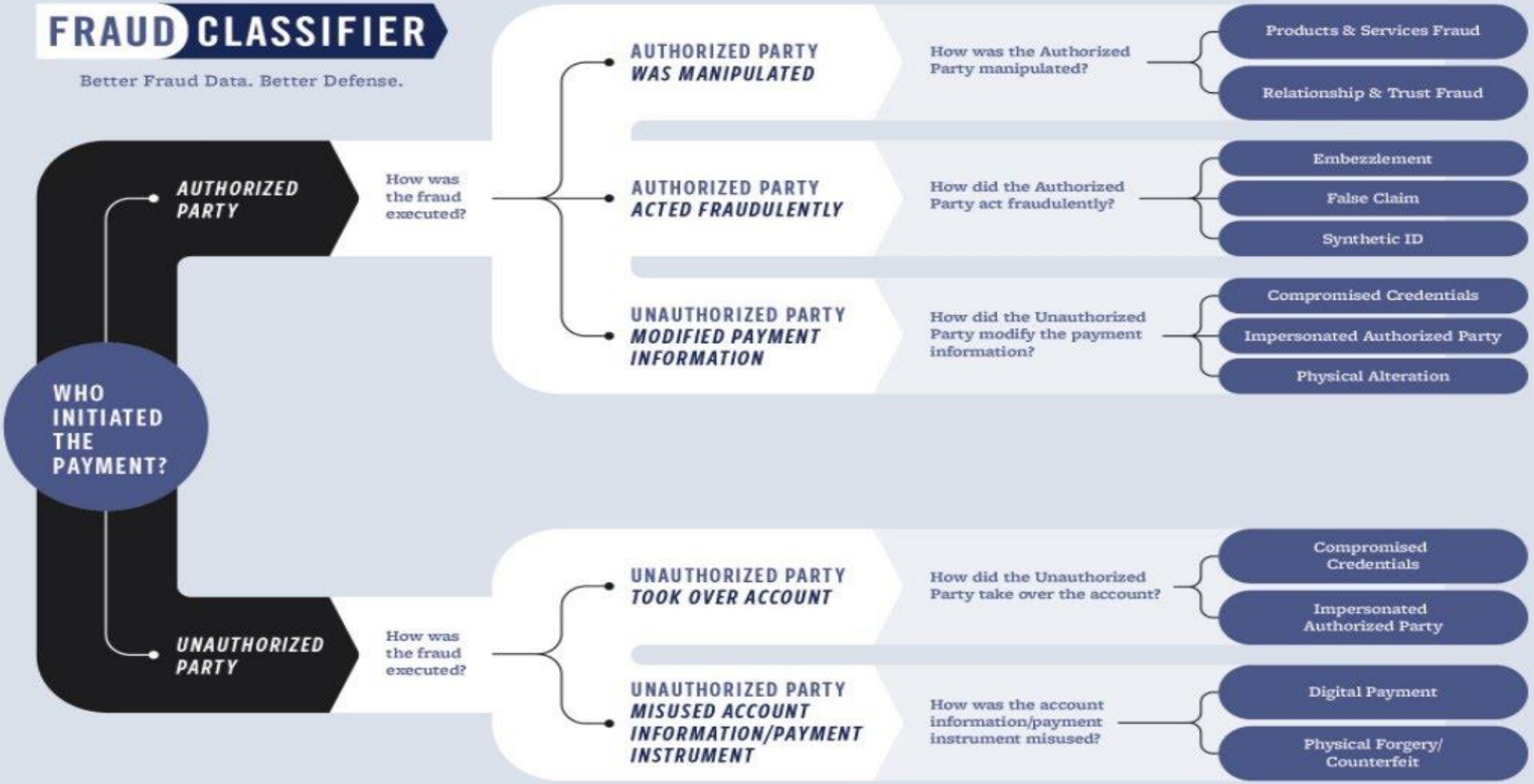
- In today's dynamic realm of payment fraud, enterprises are bolstering their defensive strategies through a comprehensive three-pronged approach. This includes the implementation of a sophisticated Rules Engine, the utilization of Machine Learning algorithms, and the application of Link Analysis techniques using Graph Networks.

A refined rules engine

- They allow for quick interventions, can be set to counteract emerging threats, and can be fine-tuned to allow for business changes and good customers. However, the power of rule-setting comes with the responsibility to use it wisely, necessitating safeguards like impact tests and expert oversight.

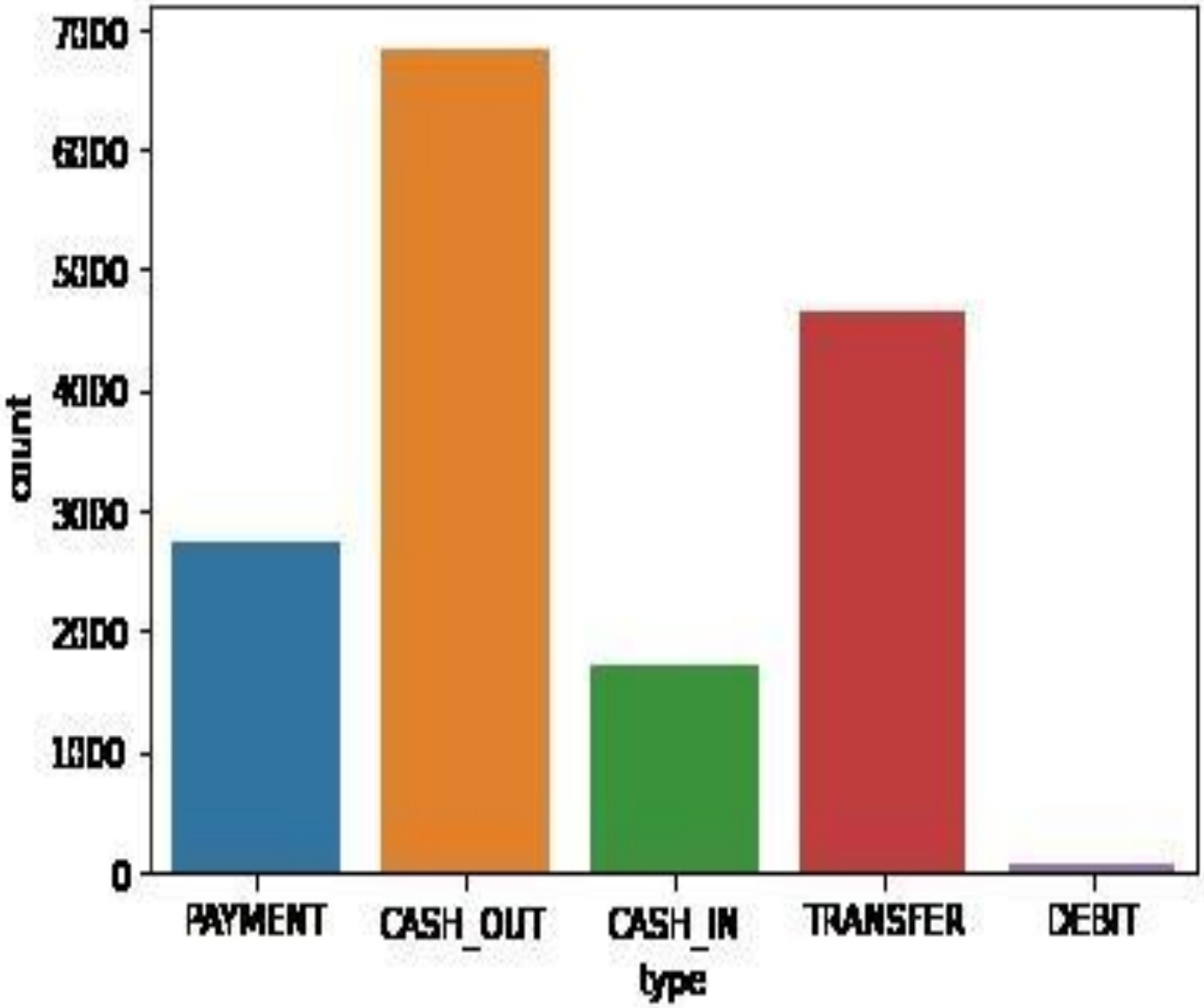
FRAUD CLASSIFIER

Better Fraud Data. Better Defense.



The FraudClassifier℠ model was developed by a cross-industry work group to provide a consistent way to classify and understand how fraud occurs across the payments industry. The FraudClassifier model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for

RESULTS



Conclusion

- Online payment fraud detection is a critical aspect of ensuring the security and integrity of digital transactions. With the increasing prevalence of online transactions, fraudsters have become more sophisticated, making it imperative for businesses to employ robust fraud detection mechanisms.
- However, while technological solutions play a crucial role, it's essential for businesses to implement a multi-layered approach to fraud prevention, including transaction monitoring, user authentication, and continuous evaluation of risk factors.

FUTURE WORKS

- Machine Learning and AI: Continued refinement and utilization of machine learning algorithms and artificial intelligence to enhance fraud detection accuracy and efficiency. These technologies can analyze vast amounts of data to identify patterns and anomalies indicative of fraud.
- Behavioral Analysis: Deeper analysis of user behavior patterns to detect fraudulent activities based on deviations from normal behavior. This could involve factors such as transaction frequency, timing, location, and spending habits
- Biometric Authentication: Integration of biometric authentication methods, such as fingerprint or facial recognition, to add an extra layer of security and reduce the risk of unauthorized access to accounts.
- Real-Time Monitoring: Development of real-time monitoring systems capable of detecting and preventing fraudulent transactions as they occur, rather than relying on post-transaction analysis.

REFERENCE

https://www.geeksforgeeks.org/online-payment-fraud-detection-using-machine-learning-in-python/

- *https://www.ravelin.com/insights/online-payment-fraud*

- *https://www.kaggle.com/datasets/rupakroy/online-payments-fraud-detection-dataset*