Quinte Financial Technologies®

Whitepaper

PAYMENT SCAMS – AI TO RESCUE

Quinte Financial Technologies

19 Fulton St, NYC, NY 10038, USA

www.quinteft.com

Contents

Executive Summary

The digital transformation in banking, driven by client demand, has led to the rise of real-time payments and instantaneous fraud. In 2023, "Imposter Scams" were the most reported fraud type. Financial institutions are investing more resources to combat financial crime, which also implies a more significant burden on resources. Traditional banking approaches often fall short in managing risk, and some legacy systems need to meet compliance, monitoring, and risk management standards. The real-time nature of transactions and the speed of fund transfers pose a severe problem if these funds are fraudulent. Therefore, banks need robust data science capabilities, reliable data sources, and Anti-Money Laundering (AML) experts to balance security with efficiency.

Scams pose a significant threat in the banking sector, with fraudsters employing various techniques to deceive individuals and gain access to their personal and financial information. These methods include SIM swaps, vishing/phishing links, lottery scams, fake loan websites and digital apps, sharing confidential information, and unknown calls/emails/messages. All these approaches mimic legitimate transactions, making it challenging for customers to prove they've been defrauded. As a result, banks often deny such claims based on their terms and conditions. Understanding these tactics is crucial for individuals and banks to safeguard against these financial frauds.

Traditional rule-based systems in the financial services industry face significant challenges in combating fraud. These systems struggle with limited adaptability to evolving fraud tactics, detection of complex fraud schemes, management of diversified digital entry points, high rates of false positives, and scalability issues with increasing transaction volumes. As a result, there's a pressing need for more sophisticated and adaptable solutions to enhance fraud detection and prevention.

Financial institutions can leverage artificial intelligence (AI) and machine learning (ML) to address the challenges of fraud detection. These technologies offer adaptability, real-time analysis, and automation, enhancing the capabilities of banks and credit unions in detecting and preventing fraudulent activities. Essential techniques include anomaly detection, predictive analytics, network analysis, text analysis, real-time detection, and adaptability. Specifically, a combination of anomaly detection, network analysis, and text analysis can effectively identify and prevent imposter scams. These techniques flag unusual account activity, identify suspicious transaction patterns, and highlight potential scam indicators in text data, providing a comprehensive and adaptable approach to fraud detection.

Introduction

Unfortunately, bank accounts and payment scams are a common way for criminals to access people's personal and financial information. In 2023, the Federal Trade Commission received more than 2.6 million fraud reports from consumers, 48% of all reports. Scammers employ various methods to trick individuals into giving up sensitive information like bank account numbers and passwords or induce them to do account-to-account money transfers. The top fraud reported by FTC was "Imposter Scams," with a whopping 854K reports. So, about 1 in 5 people lost money to imposter scams. These scams include people falsely claiming to be a romantic interest, the government, a relative in distress, a well-known business, or a technical support expert to get a consumer's money.

Banks of all asset sizes have either adopted digital services or are in the process of upgrading their technology solutions in core banking and payments. Client demand is shaping the evolution and future of financial services. While going digital, financial institutions need to tread cautiously, as the same digital solutions make it easier for scamsters to contact customers directly.

The advent of real-time payments has brought the simultaneous rise of instantaneous fraud. The potential for gain and loss in this new landscape is staggeringly large. FIs must ensure that authorization checks, fraud, and Anti-Money Laundering (AML) controls do not delay payments. However, the volume of data that must be processed for each payment to safeguard against illicit activities is substantial.

Financial institutions are increasingly allocating resources to combat financial crime. This development is a double-edged sword. While it enhances security, it also implies a greater burden on resources. Intelligent allocation of these resources involves minimizing the disruption caused by legacy systems and finding ways to work around them.

Traditional banking approaches, which are rules-based and scenario-based, may need to improve in managing risk, especially in the accuracy of scam detection. Moreover, some legacy systems must meet compliance, monitoring, and risk management standards. As per McKinsey, transaction monitoring is a critical area ripe for significant improvement. Firms require AML experts, robust data science capabilities, and reliable data sources to achieve this.

The crux of the challenge lies in the real-time nature of transactions and the speed at which funds can be transferred. If these funds are fraudulent or criminal, the fact that they can be dispersed to multiple accounts worldwide in seconds poses a severe problem for banks. The increasing global adoption and integration into real-time payment systems make this an even more pressing issue. money.

Types of Scams

Scams are a significant concern in the banking sector, and understanding their modus operandi is crucial for safeguarding against financial fraud. Here are some standard techniques used by scamsters:

SIM Swaps

Scamsters may trick mobile network operators into transferring customer/member phone numbers to a new SIM card they control. They can intercept SMS-based authentication codes once they can access the phone number.

Vishing/Phishing/SMS Links

Scammers use phone calls or emails to impersonate bank officials, urging customers or members to click on fraudulent links. These links lead to fake websites that steal login credentials or personal information.

Impersonation Scams on Zelle

A fraudster impersonates a friend, family member, or someone the customer trusts. They might claim they urgently need money and ask customers to send it via Zelle.

Lottery Scams

Scamsters claim that the customer/member has won a lottery or prize and ask for payment or personal information to release the winnings.

Fake Loan Websites and Digital Apps

Scammers create phony loan platforms or apps, enticing customers/members with attractive loan offers. Victims end up paying fees without receiving any loan.

Romantic Scams on Zelle App

Scammers exploit emotions by pretending to be interested in a romantic relationship. They build trust and then request money through Zelle.

Sharing Confidential Information

Scamsters manipulate victims into revealing confidential details (passwords, OTPs, PINs, CVVs) by creating urgency (e.g., blocking unauthorized transactions).

Unknown Calls/Emails/Messages

Customers and members should exercise caution when dealing with unknown contacts claiming to be bank officials, government representatives, or insurance agents.

Impersonation on social media

Scammers impersonate banks or customer service representatives on social media platforms and trick customers into sharing information or making payments to third parties.

As can be seen, all the above approaches are in the guise of legitimate transactions, as the customer/member themselves initiate those. When customers/members realize they have been defrauded, it becomes extremely difficult for them to prove otherwise, and the banks generally have terms and conditions in place to deny such claims.

Challenges in Traditional Rules-based Approach

Frauds in financial services are an ever-increasing phenomenon, and cybercrime generates multimillion-dollar revenues. Even a tiny improvement in fraud detection rates would generate significant savings. However, traditional rule-based systems serve the purpose in their own way. However, when it comes to scam fraud, the fraud algorithms and scorecards need to be segregated, and banks/credit unions need to work on a ground-zero approach. Let's explore some of these challenges:

Limited Adaptability

Rule-based systems rely on predefined rules. These rules are often static and cannot quickly adapt to new fraud patterns or variations. As fraudsters evolve their tactics, rule-based systems need help to keep up.

Complex Fraud Schemes

Fraudsters are becoming more organized and sophisticated. They exploit system vulnerabilities through targeted hacking, account takeover, and other methods. Traditional rule-based systems may not be equipped to detect these complex fraud schemes effectively.

Diversified Entry Points

As businesses digitize across their value chains, the attack surface for fraudsters widens. Social media, e-commerce platforms, retail transactions, rideshares, lodging services, and other entry points provide ample opportunities for exploitation.

False Positives

Rule-based systems can generate false positives, flagging legitimate transactions as potentially fraudulent due to rigid rules. This can cause inconvenience to customers and impact user experience.

Scalability

As transaction volumes increase, rule-based systems may need help to efficiently handle the sheer volume of data.

Technology to the Rescue – AI

Financial institutions are turning to artificial intelligence (AI) and machine learning (ML) to address the abovementioned challenges. ML algorithms can learn from historical data and adapt to changing fraud patterns without relying solely on predefined rules. Real-time analysis using ML models allows for more effective identification of risky transactions.

A novel AI-based fraud detection system combines data science and machine learning. It preprocesses transaction data and trains predictive models periodically (batch layer).

Simultaneously, it handles real-time fraud detection based on new input transaction data (stream layer). This architecture supports fraud analysts and automates detection processes.

AI and machine learning models can significantly enhance the capabilities of banks and credit unions in detecting and preventing scams/fraudulent activities. Here are the various ways:

Anomaly Detection

Machine learning models can be trained to recognize 'normal' behavior based on historical transaction data. Any deviation from this 'normal' pattern can be flagged as a potential anomaly, which could indicate fraudulent activity.

Predictive Analytics

AI can predict future fraud trends based on existing patterns and trends. This proactive approach allows financial institutions to stay one step ahead of fraudsters.

Network Analysis

AI can analyze the relationships between different entities (like account holders, their geographical locations, and transaction types) to identify complex fraud patterns that would be difficult to detect manually. This type of analysis is critical to all scam frauds, which otherwise appear legitimate to the average eye.

Text Analysis

AI can analyze text data (like customer complaints or transaction descriptions) to identify potential fraud indicators.

Real-time Detection

With the ability to process and analyze data in real-time, AI can detect fraudulent transactions almost instantly, allowing banks to react quickly and prevent potential losses.

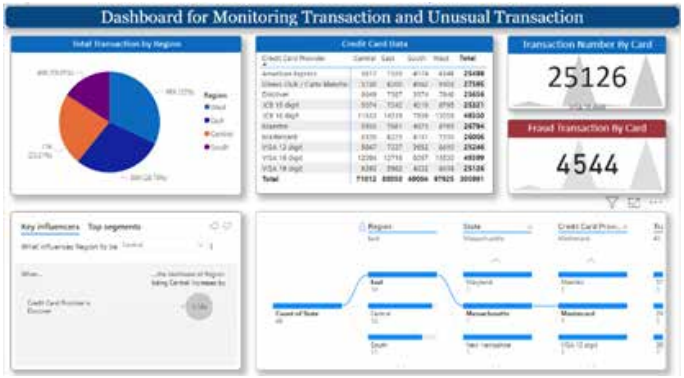
Adaptability

As fraudsters change tactics, machine learning models can adapt and learn from new fraud patterns. This makes them more effective than traditional rule-based systems that can become outdated.

Of the above-listed approaches, a combination of Anomaly detection, network analysis, and text analysis could provide a formidable solution to identify and prevent imposter scams and fraudulent activities.

Any deviation from the usual pattern is flagged as an anomaly. In the context of imposter scams, anomalies could be unusual account activity, such as large withdrawals or transfers, frequent password changes, or login attempts from unusual locations. These could indicate that an imposter has accessed a customer's account. Network analysis can help identify patterns that are indicative of fraudulent activity. For example, if an account suddenly starts transacting with a new set of accounts or a sudden increase in the volume or frequency of transactions, these could be signs of an imposter scam. Text mining could be used to analyze customer complaints or transaction descriptions for keywords or phrases commonly associated with imposter scams. For example, phrases like "prize money," "lottery win," or "urgent payment request" could indicate a potential scam.

Combining these three techniques makes it possible to create a robust system for detecting and preventing scams that leverage fraud algorithms and risk scorecards that determine the potential red flags and notify bank/credit union personnel of probable scams. The risk scorecard can also provide additional valuable data points for specific scam cases to ascertain abnormal behavior in the customer transaction. A robust monitoring, analysis, and reporting solution can help banks/credit unions tackle scams more efficiently and complement human efforts. Anomaly detection can flag unusual account activity, network analysis can identify suspicious transaction patterns, and text mining can highlight potential scam indicators in text data.



Together, they provide a comprehensive approach to fraud detection that can adapt to changing fraud patterns and help protect customers from imposter scams. It's important to note that while these techniques can significantly enhance a bank's fraud detection capabilities, they should be used in conjunction with other measures, such as secure authentication methods and customer education, to provide the most effective defense against imposter scams.

Conclusion

While traditional rule-based systems have served their purpose, they face limitations in today's dynamic digital landscape. The existing fraud scorecards won't help in culling scams. A complete makeover is the need of the hour. Adopting AI methodologies allows financial institutions to stay ahead of evolving fraud tactics and protect valuable assets more effectively.

In conclusion, adopting AI and machine learning in fraud detection can significantly improve accuracy, efficiency, and adaptability. It's a powerful tool that can help financial institutions protect themselves and their customers from the ever-evolving threat of scams. However, it's important to note that while AI can significantly enhance fraud detection capabilities, it doesn't replace the need for experienced human analysts to interpret the results and make informed decisions. It's a tool that augments human capabilities, not replaces them.

About the Authors

Sriram Natarajan

President at Quinte Financial Technologies

Sriram has over 30 years of experience in financial services for credit unions and payment processors. Sriram's extensive experience in the credit and risk industry includes positions with several highly respected organizations, including American Express, HSBC, the National Bank of Kuwait, and GE Money. He holds several professional titles, including Certified Public Accountant, Chartered Global Management Accountant, and Certified Fraud Examiner.

Paresh Ashara

Vice President at Quinte Financial Technologies

Leading the Data Analytics service line. He brings over 25 years of IT services and product engineering experience in the BFSI vertical. He is passionate about data management and analytics and takes an active interest in discussing business solutions with clients and sharing knowledge with academia. He can be reached at paresh.ashara@quinteft.com.

Quinte Financial Technologies
19 Fulton St, NYC,
NY 10038, USA

(646) 813-0694

info@quinteft.com

www.quinteft.com