A Study on Banking Frauds Identification and Prevention

Dr. K. Singaravelu
Associate Professor, Principal , Department of Commerce
CBM College, Kovaipudur, Coimbatore

R. Dhilip
Research Scholar, Department of Commerce
CBM College, Kovaipudur, Coimbatore

OPEN ACCESS

Volume: 13

Special Issue: 1

Month: March

Year: 2025

E-ISSN: 2582-6190

Citation: Singaravelu, K., and R. Dhilip. "A Study on Banking Frauds Identification and Prevention." *ComFin Research*, vol. 13, no. S1-i2, 2025, pp. 150–55.

DOI: https://doi.org/10.34293/commerce.v13iS1-i2-Mar.8754

Abstract

Bank fraud is utmost determined questions for monetary associations, whose clients face and constitute a severe risk to altogether involved parties. Fraud can be primarily caused by flawed incentive mechanisms for employees due to a decentralized lack of high-level management oversight. Conspiracy with emoloyees, business debtors and third-party agents.; weak controlstructure; lack of proper tools and know-hows in place to detect early warning signals of a scam; lack of awareness of bank employees and clients; and lack of coordination among different banks in India and abroad. Various system flaws and the evolution of legal reporting methods were thought to be some of the primary causes of fraud and non-performing assets. The banking industry is also implementing measures including tightening bank regulations and control, bolstering financial associations in line with the best performance and customer service in the world, and utilizing the newest technology for fraud detection. It contributes to lower morale.

Keywords: Bank, Fraud, Prevent, Customers

Introduction

The usage of e-commerce platforms and the different e-transactions carried out over them are essential to modern commerce. Because of its many benefits, including reduced fees, improved customer support, and quicker processing times, online banking has grown in popularity. Customers are also very concerned about security when it comes to online banking. Many consumers are concerned about their financial security as a result of the increase in fraudulent activities. Banks would create scamfinding systems that can identify questionable transactions in order to stop these kinds of activities.

Systems that detect fraud on the Internet classify transactions into two categories that are harmful to fraud and health. The system uses the comparison method to check the transaction Effective fraudulent detection systems candetect high risk transactions to prevent them. Systems based on rules are also used to prevent fraud. Based on the rules, the system uses the preliminary rules to identify fraudulent transaction patterns.

Since the economy was liberalized in 1991, the Indian banking industry has seen substantial expansion and transformation. The banking sector faces a unique mix of issues with regard to corporate governance, financial crisis, and ethical behaviors, despite being generally well-regulated and overseen. Financial fraud cases have been often reported in India in recent years. India have traditionally been dismissed as a necessary part of conducting business, since deregulation, their regularity, difficulty, and price have skyrocketed, raising severe concerns for authorities like the RBI.

Fraud under the Companies Act, 2013

The 2013 Companies Act addresses issues pertaining to business fraud. Vizibland may carry on in the future. The issue, conduct, exclusion, demolition of facts, or misuse of positions perpetrated by a corporation or entity, by any means, by a person or another person with whom you agreed, are all considered forms of fraud under section 447. Deception or violation of any postponed interest, whether it be from the company's, its shareholders', its creditors', or others' interests, is not an illegal profit or loss.

Review of Literature

Uppal 2008, it says that the transformation takes place in Indian banks according to various parameters.The contours of the banking service dynamically changed the face of banking services, and banks go to an electronic banker, satisfied with various electronic channels and their services, but the lack of awareness is a serious obstacle to the spread of more electronic services.

According to the report, Singh (2012) lists the many phishing strategies that con artists employ. ICICI Bank first reported a number of incidents, followed by UTI Bank and National Bank of India. There are numerous instances of attacks against legitimate websites in India.

In 2013, Parameshwara, G. The GopalKirshna Committee, established by the RBI in 2011, suggests a particular plan that all banks implement in order to reduce the risk of fraud and to routinely monitor for it.

In this paper, Anita (2008) discusses credit card frauds and how to avoid them. Credit cards, debit cards, and smart cards have given money a new form by providing quick liquidity, a steady flow of payments, and additional convenience. Although there are many advantages to using these cards, there is also a significant risk of suffering significant losses.

Since its inception in 2001, Path has examined the difficulties and consequences of the new technology for banks. The earlier manual procedures of creating vouchers, etc., are gradually being automated there, saving a great deal of time and work, as talent has completely changed the way banks operate.

Types of Online Frauds

Advance payment fraud

Beforehand, fraud scams persuade victims to pay to receive what is valuable to the victims, but they do not provide anything to the victims.

Phishing

Phishing occurs when fraudsters utilize email or fraudulent SMS to lure users to bogus websites, wherein users are asked to provide personal, financial, and confidential data like account numbers, passwords or transaction details [10]. For phishing, the emails or SMS are sent by fraudsters on behalf of e-shops, credit card industries or banks, requesting users to update or change their profile/ account defaults. The phishing SMS/email texts are persuasive, instigating users to believe in their

origin. In these texts, the hyperlinks and logos of companies, mirroring the original ones, are used to enhance user trust. When the user proceeds through such websites and enters the requested personal details in those links, the fraudsters smartly take advantage and utilize those details for their vicious needs.

Online Auction Fraud

Online auction (OA) fraud is an important variety of fraud. This sort of fraud mostly affects clients/users during the bidding activity performed online for products and goods. In this fraud, fraudulent transactions occur within the framework of an online auction website. In other words, this fraud is generally committed through different auction sites. Such auction sites bring about a hundred million goods together for trade, with multiple buyers and sellers.

Online Investment Theft/Fraud

Trick frequently convinces online shoppers to invest specific sums of money in different businesses that do not exist overseas in order to commit online investment theft. The method suggests that online buyers purchase shares of such a company as an alternative. A scammer who is such a kind of fraudulent uses advertising, investment voting paper, chat and massemails to attract customers. They use the method of pump& dim, where the individual is associated with others who contain internal information about the organization specified on the securities exchange. Because of this, this person should buy a promotion because he expects fast and good income. At a new high price, a scam drops the company's shares and gains short term growth. If stock prices decrease, Trickster gains profits due to changed customers.

Card Testing

Someone receives information about the card in a malicious network and obtains access to card number throughtheft.Despite the number of cards, they don't know, but the transaction be completed successfullyusing the map number or b. Therefore, fortesting, a scammer first studies whether he can perform a few tests and use the map number to perform the entire transaction. After understanding that the cardworks, the scammer starts an expensive purchase. Finallyinitial small test strategy for purchasing is often unknown. The victims understand that the scammer was deceived after making a big purchase.

Clean Fraud and Chargeback Fraud

Clean fraud is executed with the credit card that is filched from an authentic customer and is employed to make e-purchase. Here, the card holder's details and filched card is employed to perform the fraud which appears like a licit purchase done by a valid customer. In chargeback fraud, also called friendly fraud, the user keeps the products/goods purchased online, but still requests for a repay stating payment being done twice or purchase never done or item never received. Chargeback frauds often occur owing to hacked payment data and filched credit cards. Fraudsters employ this data for performing fraudulent actions or purchases and even shipping goods to their address or to the tampered address

Triangulation fraud

In triangulation fraud, the trickster establishes a bogus online shop providing products/goods at low prices. This sort of fraud involves three participants namely bogus online store, stolen data and unsuspecting user. Here, once the user buys the items, the bogus merchant immediately sneaks user's card details. The chief motive of creating web shops here is to gather credit card information of users making purchases or visiting these sites. The fraudster after acquiring card details, cancels the received payment on user's card

Payment Fraud

Generally speaking, fraudulent cards, stolen cards, and lost or improper credit cards are used for payments. The cardholder must pay the bill, and payment, fraud, and tricksters must finish the payment. The majority of fraudulent transactions that do not require the actual presence of cards take place on websites that are vulnerable to fraud.

Interception Fraud

In interception fraud, after placing orders, the package is intercepted by fraudsters and goods are taken by fraudsters for themselves. In this sort of fraud, fraudsters may ask the company's client service representative to change the package's (order) address before shipping that package. Here, fraudsters aim to obtain the goods/package while the package payment is already done by the victim. Sometimes, fraudsters may even contact the courier (shipper) to reroute the goods to their address.

Bank Fraud Detection and Prevention Technology

Artificial Intelligence: Conventionally, banks and other financial organizations employ rules-based engines to detect rogue transactions, which are produced by a number of swiftly occurring new accounts or transactions involving risky IP addresses. Solutions for fraud monitoring have received our endorsement.

1. Heart code. This means that it cannot adapt to developing threats
2. Binary. This means that it cannot absorb the complexity of various input variables and is incorrectly incorrect.

AIbased fraud monitoring systems allow large amounts of data to be absorbed and analyzed as large amounts of transactional banks per day record fraudulent activities and fraudulent activities in real time.

- Machine learning: This is a powerful tool to prevent the morale of the banking industry. Machine training allows you to learn from behavioral data, consortium data and other internal and external data sources, and thus adapt. As a result, banks can better explore them in more and more difficult fraudulent environments and more actively protect their customers and assets..
- Biometric authentication: Bio authentication is an identification method based on the uniquephysical characteristics of customers, suchas voices, face functionor fingerprints for testing personality. These characteristics are known as biometric data.
- Two-factor and/or multi-factor authentication: These methods involve asking a bank customer to present multiple pieces of proof to verify their identity. In order to develop a comprehensive fraudulent strategy, other approaches such as biometric authentication must be used in addition to the fairly conventional security measures like 2FA and MFA.
- Advanced analytics: Every day, hundreds of transactions are handled by financial institutions, and each one produces data. Customer data and transactions may be analyzed with great power using advanced data science techniques. This gives the bank a 360-degree view of the entire business, boosts operational effectiveness, and helps identify predictive fraud.

Preventive Measures for Online Frauds

Protection of online transactions from fraudulent actions is possible through recognizing various fraudulent activities. Fraud preventive methods can lower the fraud threat and assure that fraud does not affect the business. Some significant preventive measures against fraud occurrence include:

Conducting Regular Site Security Check

Users should regularly conduct site security checks to find flaws, if any, in their security configuration/ framework before fraudsters target and identify them. These security audits conducted often can aid in a) identifying whether communication or transaction during e-purchase activity is properly encrypted, b) confirming whether the secret codes employed for File Transfer Protocol (FTP) access, database and admin accounts are robust enough, c) confirming whether purchase making website/application is security standard compliant and d) confirming whether the site or transaction platform is being regularly scanned for malware

Using Address Validation Service

Credit card issuing banks typically render an address validation service for detecting dubious real-time card transactions and preventing card frauds. An address validation service audits whether the transaction card user's billing address matches the billing address details of cardholder. This validation is executed for authorizing the card transaction. In case of address mismatch, system either flags the transaction or declines it and performs further investigation. Thus, this service can prevent fraudulent transactions.

Utilization of Device Identification Software

Generally, device identification software aids in identifying and tracing the devices which request a transaction. The software of this type is valuable for ascertaining any transaction's authenticity and can trace the transaction's source in case of doubt of fraudulent activities.

Use of Smart Geo-Location

The smart geo-location technology assists in tracing and tracking user's location during transactions. The fraudulent action tracing through geo-location can easily identify individuals at any place/location when they are making any smart transaction. The smart geo-location technology is also productive when a trickster tries to hide location or identity.

Using Hypertext Transfer Protocol Secure (HTTPS)

The HTTPS is basically a secure HTTP version, which exchanges information between the user's web browser and an e-purchase store. It encrypts information for protecting sensitive information like user names, card numbers and addresses, thereby securing confidential user details from fraudsters. Utilization of HTTPS prevents fraudsters, hackers and criminals from easily viewing the user's transaction details

Utilization of Digital Signatures

Digital signatures are mainly considered as the digital tantamount of conventional handwritten signatures [15]. Adoption of digital signatures for many online transactions are helpful for avoiding frauds, this is chiefly because they are tedious to forge. As these signatures employ cryptographic methods, fraudsters cannot easily forge them

Use of Reverse Lookup Mechanism

The reverse search mechanism is primarily based on public data (stored in state records). This mechanism includes telephone data and address reviews. This is provided by users regarding the source of third party providers of public documents/records.This mechanism thus verifies potential user's particulars with user's records in government database or public file. Its efficacy is chiefly dependent on the presumption that public databases are unfeasible to be tampered or misrepresented.

Card Security Methods

Checking the verification number can ensure the card's individuality and cardholder's identity. This can ratify that the individual claiming to be the card's owner is the real owner and is having the transaction card [16]. Along with the card's verification number, cardholder's other details like address, location are also utilized. This can prevent transaction card frauds executed online, particularly when fraudsters have somehow extracted details using the user's history

Importance of AI and Machine Learning in Bank Fraud Detection

These days, artificial intelligence (AI) and machine learning are crucial in helping banks address the risk of fraudulent activity. However, it's crucial to remember that this benefits banks in a number of ways.

First, we can observe the model with the large quantity of data that banks employ thanks to graphical analysis, clustering identification, and anomaly detection techniques. This technology is crucial since it makes it impossible to conduct a significant quantity of analysis by hand.

Second, automation enables banks to increase their operational speed. Banks are able to cover more causes than they were previously able to by automating the creation of warnings and reports on suspicious activity (SRAS) based on a particular approach to the organization according to risks. Clarifying more cases faster and minimizing the amount of time spent on false works are two ways that teams might meet criteria.

Third, banks are able to handle fraud in a more adaptable manner thanks to AI and autonomous learning. AI enables the bank to grow and advance at a pace commensurate with criminal activity by enabling compliance orders to incorporate additional data sources and establish their own rules to detect models. Better software to identify bank fraud

To deal with the huge volume, diversity and ferocity of attempts at fraud, which they are subjected to daily grounds, banks need powerful AI and intellectual software. When checking suppliers to detect fraud, banks can choose the priorities of decisions that offer the following opportunities:

- Fast integration of media unfavourable coatings, sanctions lists, lists of politically exposed people (PEPs) and profitable owners (UBOs), data for connections of several flows.
- A robust automatic learning model that can detect over 50 different forms of fraud across all payment rails after being educated with owner data about customers, business, and financial risk.
- Unmatched speed of assessment thanks to tried-and-true methods and opportunities that enable banks to survive in just two weeks.
- Extended opportunities, such as dynamic threshold values, identification clustering and the discovery of a graphic network to adapt to criminals, analyze related accounts and follow the means throughout the system.

Conclusion

Bank fraud is one of the utmost determined questions for financial institutions, whose customers face and constitute a severerisk to altogether involved parties.Since there is a dispersed absence of high-level managerial control, staff incentive systems that are defective can be the main source of fraud. Lack of knowledge about bank employees and customers, inability to coordinate across different banks in India and abroad, inadequate control structure; lack of the necessary tools and expertise to identify early warning signs of a scam; and collusion between employees, business debtors, and third-party agents. Various system flaws and the evolution of legal reporting methods were thought to be some of the primary causes of fraud and non-performing assets. Measures such as strengthening bank control and regulatory agenda and strengtheningfinancial associations in harmony with the world's finest performance and efficient customer service and the latest technology for effective fraud detection are also being implemented in the banking sector. It helps to reduce morale.