INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 4 AND ISSUE 4 OF 2024

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Free and Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 4 and Issue 4 of 2024 (Access Full Issue on - https://ijlr.iledu.in/volume-4-and-issue-4-of-2024/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

AN EXAMINATION OF CREDIT CARD FRAUDS – TYPES, TECHNIQUES AND PREVENTION STRATEGIES IN INDIA

AUTHOR - CHARUMATHY B* & MS. T. VAISHALI**, LLM SCHOLAR* & ASSISTANT PROFESSOR OF LAW** AT THE TAMILNADU DR. AMBEDKAR LAW UNIVERSITY (SOEL), CHENNAI

BEST CITATION – CHARUMATHY B & MS. T. VAISHALI, AN EXAMINATION OF CREDIT CARD FRAUDS – TYPES, TECHNIQUES AND PREVENTION STRATEGIES IN INDIA, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (4) OF 2024, PG. 909-915, APIS – 3920 – 0001 & ISSN – 2583-2344.

ABSTRACT

Credit card fraud poses a significant challenge for India, with a growing number of instances involving unauthorized credit card use and financial losses emerging as a major concern. The paper explores different approaches to detect and prevent credit card fraud through smart data analysis, AI-powered machine learning, real-time transaction monitoring, as well as discussing prevention strategies like implementing two-factor authentication (2FA), secure payment systems, and educating consumers. Through the use of these tools and processes, banks, customers and beneficiaries can work together to minimize the risks of credit card fraud while also improving overall security measures.

Keywords: Credit Card, Frauds, Tools, Techniques, Prevention, Cyber, Transactions.

INTRODUCTION

In the present day, as digital services become more prevalent, the challenge of credit card fraud poses a significant concern for both individuals and businesses. With the rise in credit card usage in India, there has also been an increase in the cunning methods employed by criminals to pilfer funds from the financial system. The repercussions of these illicit activities extend beyond mere financial loss, potentially eroding individuals' confidence in banks and similar financial establishments. This particular matter is crucial as addressing it would effectively safeguard the integrity of financial transactions.

Efforts must be made to effectively combat credit card fraud, which can be achieved through a variety of methods. For example, the sophisticated technology of machine learning (AI) could be employed to examine the ways in which individuals utilize their cards. It's crucial to enhance security by implementing biometric authentication methods like fingerprint or facial recognition technology. Moreover, individuals should receive education on the tactics employed by scammers in order to enhance their self-protection.

Simply put, tackling credit card fraud in India requires a combination of advanced technology and engagement from consumers. A system that prioritizes security and education can help minimize the chances of credit card fraud occurring. By collaborating, banks, government agencies, and consumers have the power to cultivate a secure financial landscape, boosting confidence in digital payments and bolstering the economy.

OVERVIEW OF CREDIT CARD FRAUD IN INDIA

The surge in digital transactions in India has unfortunately paralleled a significant rise in credit card fraud cases, creating pressing concerns for consumers and financial institutions alike. As the adoption of e-

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

commerce and online banking expands, cyber criminals are increasingly exploiting vulnerabilities within these systems, employing sophisticated techniques that evade traditional security measures. Major contributing factors include inadequate awareness among users regarding safe online practices and the lack of stringent regulations in cyber security frameworks, which puts individual consumers and national security at risk[1392]. Moreover, as new technologies such as AI and digital payment platforms develop, they can either enhance security or provide new avenues for fraud depending on their implementation. Consequently, it is imperative for India to bolster its cyber security protocols and educate users on effective preventive measures. Such initiatives will be essential for safeguarding financial transactions and reducing the growing incidence of credit card fraud.

TYPES OF CREDIT CARD FRAUDS IN INDIA:

The escalating sophistication and diversity of credit card fraud in India pose significant challenges for both consumers and financial institutions. Various types of fraud, such as phishing, skimming, and card-not-present (CNP) fraud, exploit technological advancements and human vulnerabilities to gain unauthorized access to credit card information. Fraudsters employ a range of techniques, from deploying malware to intercept sensitive data to using social engineering tactics to deceive individuals into revealing their card details. The rapid evolution of these fraudulent activities necessitates continuous vigilance and the implementation of robust security measures to safeguard against potential threats. Understanding the different types of credit card fraud is essential for developing effective prevention strategies and protecting the financial well-being of consumers.

Card-not-Present (CNP) Fraud:

Card-Not-Present (CNP) Fraud refers to credit card fraud where a transaction is carried out without the use of the physical card. This occurs mostly during online shopping, orders over the phone, or through mail orders[1393]. The card cannot be physically verified, making it easier for fraudsters to use stolen card details to make illegal purchases.

Card Skimming:

Card skimming is a form of credit card fraud where, using a device called the card skimmer, criminals are stealing card information. These skimmers can be attached to ATMs, POS terminals, or gas pumps. When you swipe your card through a compromised machine, it captures and stores your card details to make unauthorized purchases or counterfeit cards[1394].

Phishing and Vishing:

Phishing is when scammers use emails or messages that impersonate actual companies. They fool the victim into clicking harmful links or opening risky files, which end up stealing personal information.

Vishing is when the fraudsters call people posing as organizations they are trusted by, such as banks or even government agencies. They then try to trick them into revealing sensitive information such as passwords or credit card numbers.

Both phishing and vishing employ social engineering to exploit human vulnerability in terms of trust and fear, which can result in unauthorized access to a person's financial accounts or even personal information, thereby giving rise to serious consequences.

Lost or Stolen Cards:

This is the age-old trick of physically stealing a

[1392] Alok Mishra, Yehia Ibrahim Alzoubi, Memoona J. Anwar, Asif Qumer Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations", 2022, pp. 102820-102820

[1393] What are card-not-present (CNP) transactions, Available at: https://stripe.com/in/resources/more/what-are-card-not-present-transactions, (visited on Nov. 13, 2024)

[1394] *What is Credit Card Skimming and How to Avoid It?,* Available at: https://www.airtel.in/blog/credit-card/what-is-credit-card-skimming-and-how-to-avoid-it/ (visited on Nov. 13, 2024)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

credit card from a person's pocket. This kind of credit card fraud implies that your credit card was taken from you without your authorization or that you lost it. In this case, someone may use your credit card until you report the loss and get the card blocked from your bank.

Application Fraud:

Application Fraud occurs when an individual lies or cheats on an application to get something they're not supposed to have. This is common in industries that rely on online applications for things like creating accounts, getting loans, or being approved for credit.

Fraudsters may use fake identities, fake documents, or false information about their job or income to deceive banks and other financial institutions into giving them loans, credit cards, or other financial products[1395].

Keystroke Logging:

Hackers use malicious software to capture credit card details as you type them on your computer. Keystroke logging, commonly referred to as key logging, is when your every keystroke of your keyboard is monitored surreptitiously without even letting you know about the tracking. This is generally executed with the help of hazardous software or secret devices often called key loggers[1396]. These installed key loggers siphon all critical information, such as log-in passwords, credit cards, and private messages between friends. This critical piece of information can then be used for identity thefts, financial frauds, and unauthorized access to one's personal accounts.

TOOLS AND TECHNIQUES USED IN CREDIT CARD FRAUD

In the battle against credit card fraud, many tools have been created to find fraudulent activity. One of the most important tools is advanced machine learning algorithms that can analyze large amounts of transaction data. These algorithms can spot patterns that suggest fraud by identifying unusual activity.

One research shows that the choice of the detection methods is critical for the reliability of the models, especially when dealing with imbalanced credit card fraud data. Traditional methods fail in such cases[1397]. Tools like real-time transaction monitoring also is very helpful as it immediately alerts us when there is suspicious activity. It also helps in reducing financial loss and building trust in digital transactions.

Overall, a strong tool in analysis strengthens the credit card fraud security framework necessary in India's burgeoning digital economy.

COMMON TOOLS EMPLOYED BY FRAUDSTERS

Fraudsters are known to use many clever tricks in stealing credit card information. Therefore, it is hard to prevent credit card fraud. Among these tricks, phishing has become one of the common tricks used by fraudsters in an attempt to trick people into giving their personal information, which may include credit card details. This is because the internet does not have borders, so fraudsters can operate from anywhere in the world and reach many people. Another trick is to use malware such as key loggers to steal information directly from people's computers. This is how technology can be used for good and bad purposes in online banking.

Some fraud schemes are worsened by the fact that people do not know enough about how to protect them and by the fact that companies do not have strong enough security measures. This highlights the need for better security measures to fight these common tricks. These issues need to be

[1395] Application Fraud:What is It, Examples & How to Detect It, Available at http://seon.io/resources/application-fraud/ (visited on Nov. 15, 2024)

[1396] Keystroke logging, Available at: https://en.wikipedia.org/wiki/Keystroke_logging/ (visited on Nov. 15, 2024)

[1397] Dalai, Sasanka Sekhar, Femi Godslove, Julius, Kpereobong Friday, Ibanga, Nayak, Subrat Kumar, Tripathy, Nrusingha, "Credit Card Fraud Detection Using Logistic Regression and Synthetic Minority Oversampling Technique (SMOTE) Approach", Institute for Project Management Pvt. Ltd, 2023

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

addressed to protect consumers in India's growing digital financial world.

Some of the most common tools and techniques used in credit card frauds are:

Geo location spoofing:

It is one of the tricks used by fraudsters to make the location of a transaction appear elsewhere for bypassing security checks. [1398]It uses VPNs and proxy servers in making the transaction look as though it is coming from an actual location. This will then evade detection and commit fraud undetected. It can be negated by companies using advanced location verification technology and multi- factor authentication to ensure transactions are real.

Carding bots:

These are programs used by cybercriminals to check stolen credit card information at many online websites. A criminal feed these bots stolen card details, which then go on to try to make small purchases on many websites with the hope of finding a valid card number. Upon finding valid cards, the criminals use them for greater fraudulent purchases or sell them out on the dark web. Traditional fraud detection systems will find it difficult to capture the carding bots that function extremely fast and efficiently[1399]. So, it becomes necessary for some really strong security measures that are implemented like multi-factor authentication and real-time monitoring of transactions to fight back this advanced fraud.

Fraud Fox and Multi Login:

Fraud Fox and Multi Login are sophisticated tools that cybercriminals use to automate and mask credit card fraud. Fraud Fox enables fraudsters to impersonate various devices and browsers, which makes it difficult for fraud detection systems to recognize suspicious activities. Multi Login allows the use of various accounts and devices to pass security checks and carry out unauthorized transactions. These tools greatly enhance the efficiency and effectiveness of fraudulent activities, which can be a significant threat to consumers and businesses alike[1400].

Machine learning algorithms:

Machine learning algorithms play a great role in curbing credit card fraud through massive analysis of the data associated with transactions for suspicious activity. The algorithm can then identify anomalies in real-time and flag those potentially fraudulent activities over time as it learns how fraudsters will evolve with new tactics. Through learning from transaction data, their accuracy and efficiency in detecting fraud continually improve. Implementing machine learning in fraud detection systems helps businesses stay ahead of cybercriminals and protect consumers from financial losses.

TECHNIQUES FOR EXECUTING CREDIT CARD FRAUD

There are several techniques that allow criminals to commit credit card fraud, which are a serious threat to financial security. One of the most common techniques is phishing, in which attackers duplicate authentic websites or send spam emails to dupe people into providing their personal and financial information. This technique works because of psychological manipulation of the victim, who believes he is communicating with his trusted service providers[1401]. Thus, victims unintentionally provide sensitive information that is being exploited by fraudsters for money purposes. Another technique involves skimming, which is secretly fixed in the ATMs or point- of-sale terminals to collect card

[1398] *Fraud Detection Tools,* Available at: https://chargebacks911.com/fraud-detection-tools/ (visited on Nov. 15, 2024)

[1399] *Carding,* Available at: https://www.imperva.com/learn/application-security/carding-online-fraud/ (visited on Nov. 18, 2024)

[1400] *Id.*

[1401] MADHURI, M., Sagar, U. VIDYA, YESESWINI, K., "INTELLIGENT PHISHING WEBSITE DETECTION AND PREVENTION SYSTEM BY USING LINK GUARD ALGORITHM", Institute for Project Management Pvt. Ltd, 2020

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

information while carrying legitimate transactions. Such methods not only compromise personal security but contribute to broader economic disruption because of lost businesses and mistrust towards digital transactions. In consequence, understanding these techniques is important for developing an appropriate prevention strategy against credit card fraud[1402].

METHODS OF FRAUDULENT TRANSACTIONS

With the development of technology, fraudulent transactions in India have gone a long way, hence requiring greater understanding of the methods employed by cyber criminals. One such prevalent technique is using stolen credit card information that is most often acquired through phishing attacks or data breaches whereby fraudsters use victims' personal details to make unauthorized transactions. For example, transaction data attribute manipulation is crucial in suspicious activity identification as has been observed in the financial industry where credit card fraud models, such as Logistic Regression, have an accuracy of 98%[1403]. Additionally, like the health care industry, which was discussed in previous researches, the detection of fraudulent activity within government programs, such as Medicaid, shows that fraud prevention efforts must be continually developed and improved to keep pace with the changing tactics of fraudsters[1404]. Therefore, a multidisciplinary approach involving advanced technology and data analysis is critical to combating fraudulent transactions[1405].

PREVENTION STRATEGIES AGAINST CREDIT CARD FRAUD

A holistic approach to the prevention of credit card fraud should be a balance of technological solutions and education among users. Machine learning algorithms that analyze spending patterns will help in detecting anomalies, which may be indicators of fraudulent activity. Financial institutions must prioritize customer awareness programs educating the users on safe practices such as monitoring their account activities regularly and avoiding the online sharing of sensitive information. As seen in the banking sector, where there is a sharp rise in fraud, and thus calls for a strong response, using technology while encouraging vigilant users is the need for effective prevention[1406]. By infusing innovative detection tools along with thorough education of consumers, risk towards credit card frauds can be minimized, hence keeping the integrity of Indian financial transactions intact[1407].

Credit card fraud prevention involves using a multitude of technologies with consumer consciousness. Some prevention strategies involved:

Multi-Factor Authentication or MFA:

This strategy adds another level of authentication when more than one method needs to validate the user before allowing a transaction. The methods to consider use something the user knows - password, has - Phone number, or is - biometric, which could prevent large degrees of fraud.

Real-Time Monitoring and Alerts:

Implementing systems that monitor transactions in real time and notify the cardholder of any unusual activity can help detect and stop fraud early.

EMV Chip Technology:

Using credit cards with EMV chips, which are harder to clone than magnetic stripe cards, helps reduce card-present fraud.

[1402] Somesh Kumar, "CYBER CRIME: A Review", Innovative Scientifc Research Publisher, Railway Station Road, Gandinagar, Karnataka, 2024.
[1403] *Supra* note 1.
[1404] Hillegersberg, Jos van, Müller, Roland M., Thornton, Dallas, Travaille, Peter, "Electronic fraud detection in the U.S. Medicaid Healthcare Program: lessons learned from other industries", 2011
[1405] Id.
[1406] HASIN, Madan Lal, "THE ROLE OF TECHNOLOGY IN COMBATTING BANK FRAUDS: PERSPECTIVES AND PROSPECTS", Association of Educational and Cultural Cooperation Suceava from Stefan cel Mare Universit, 2016
[1407] Id.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Tokenization and Encryption:

These technologies safeguard cardholder information during transactions by converting the data into unreadable tokens and encrypting it to make it useless if fraudsters intercept it.

Regular Account Monitoring:

Encouraging consumers to regularly review their account statements and transaction history helps immediately identify unauthorized transactions.

Consumer Education:

Educating cardholders on common types of fraud, safe online practices, and ways to recognize phishing attempts puts them in a better position to protect their information.

Address Verification System (AVS):

Verify address entered by the card owner on file against that held in the merchant's system

Behavioral Analytics:

Monitor the transaction pattern with machine learning or AI, identify and block out anomalous transactions.

Online Merchant Security Payment Gateway:

Secure online payment gateway system must be implemented and enforced that is robust and secure such that it does not succumb to fraudulent practices, therefore ensuring low levels of fraud online.

Regulatory Compliance:

It ensures compliance with industry standards and regulations, such as PCI DSS, and relates to secure best practices in handling cardholder data by businesses.

EFFECTIVE MEASURES FOR CONSUMERS AND INSTITUTIONS

In the modern digital world, both consumers and institutions must take preventive measures to prevent credit card fraud. For the individual, awareness is key; proper, unique passwords for all online transactions and frequent review of bank statements will easily alert them to any fraudulent activity. Institutions, in turn, should focus on formulating comprehensive cyber security policies. The sophistication of these cyber threats requires a holistic response to cyber security, which holds effective policy as the cornerstone that can resist these changing conditions[1408]. More importantly, consumers can rely on online transaction security in the presence of XAI in cyber defense processes, bringing about transparency and trustworthiness[1409]. The combining of individual vigilance with institutional accountability will breed a safer environment that may well minimize the possibilities of credit card fraud and safeguard confidential financial information.

THE EFFECT OF CREDIT CARD FRAUDS IN INDIA

Credit card frauds in India have significant consequences for individuals and the economy.

Impact on Individuals:

- Financial Loss: Victims of credit card fraud suffer direct financial loss due to unauthorized transactions.
- Emotional Stress: The process of reporting fraud, dealing with banks, and resolving the issue can be emotionally draining.
- Loss of Trust: Fraud incidents can erode trust in digital payment systems, making individuals hesitant to use credit cards for online transactions.

Impact on the Economy:

- Increased Costs for Banks: Financial institutions bear the costs of fraud investigations, reimbursements, and implementing advanced security measures.
- Reduced Consumer Spending: Decreased trust in digital payments

[1408] *Supra* note 1.

[1409] Zhibo Zhang, Hussam Al Hamadi, Ernesto Damiani, Chan Yeob Yeun, Fatma Taher, "Explainable Artifcial Intelligence Applications in Cyber Security: State-of-the-Art in Research", 2022, pp. 93104-93139

can lead to reduced consumer spending, affecting economic growth.

- Damage to Financial System: Widespread fraud can erode public confidence in the financial system, potentially leading to economic instability.

Addressing the Challenge:

To mitigate the impact of credit card fraud, a collaborative approach is necessary:

- Strong Security Measures: Financial institutions should invest in advanced security technologies to protect customer data.
- Consumer Awareness: Educating consumers about fraud prevention techniques, such as recognizing phishing attempts and safeguarding personal information, is crucial.
- Regulatory Oversight: Robust regulations and enforcement mechanisms can deter fraudsters and hold them accountable.
- Prompt Response: Banks should have efficient systems to detect and respond to fraudulent activity promptly.

By taking these steps, individuals and institutions can work together to protect against credit card fraud and ensure a secure digital economy.

CHALLENGES AND FUTURE DIRECTIONS IN CREDIT CARD FRAUDS

Credit card fraud in India has become increasingly sophisticated and diverse, posing significant challenges for both consumers and financial institutions. Various types of fraud, such as phishing, skimming, and card-not-present (CNP) fraud, exploit technological advancements and human vulnerabilities to gain unauthorized access to credit card information. Fraudsters employ a range of techniques, from deploying malware to intercept sensitive data to using social engineering tactics to deceive individuals into revealing their card details. The rapid evolution of these fraudulent activities necessitates continuous vigilance and the implementation of robust security measures to safeguard against potential threats. Understanding the different types of credit card fraud is essential for developing effective prevention strategies and protecting the financial well-being of consumers.

CONCLUSION

In examining the tools, techniques, and prevention measures against credit card fraud in India, one must recognize the rapidly evolving landscape of cyber threats that accompany the growth of digital transactions. Effective cyber security is not merely a protective measure; it serves as a foundational element for fostering consumer trust in online financial activities. As the prevalence of cyber-attacks increases, comprehensive protective strategies become crucial, which underscores the necessity of safeguarding information in a digitally dominated world[1410]. Moreover, the integration of Explainable Artificial Intelligence (XAI) in cyber defense mechanisms can enhance the interpretability of fraud detection systems, thereby empowering financial institutions to explain their defenses against potential threats. Ultimately, a multi- faceted approach, incorporating advanced technologies—both preventive and explanatory—is essential for combating credit card fraud and reinforcing secure transactional environments in India's burgeoning digital economy.

[1410] Dr.Yusuf Perwej, Syed Qamar Abbas, Jai Pratap Dixit, Nikhat Akhtar, Anurag Kumar Jaiswal, "A Systematic Literature Review on the Cyber Security", 2021, pp. 669-710