VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

# A COMPREHENSIVE STUDY ON CARD-NOT-PRESENT (CNP) FRAUD: TRENDS, TECHNIQUES, LEGAL FRAMEWORK AND CHALLENGES

- Hemasruthi A[1] & T. Vaishali[2]

## ABSTRACT

This research paper examines Card-Not-Present (CNP) fraud, which has grown rapidly in India as people increasingly depend on online payments and digital banking. The study explains how CNP fraud occurs without the physical card and why it has become one of the most common forms of financial cybercrime today. It discusses the major techniques used by fraudsters, such as phishing, SIM-swap attacks, database leaks, and malware, which help them steal sensitive information and carry out unauthorized transactions. The paper also highlights recent trends, NCRB insights, and industry observations that show how organised and technology-driven CNP fraud has become.

To understand the legal response, the research looks at relevant provisions under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita (BNS), 2023, along with RBI regulations that guide banks in safeguarding digital payments. Despite these laws, several challenges remain in detection, investigation, and prosecution due to technical limitations, consumer unawareness, and cross-border networks. The paper concludes that a combination of stronger authentication systems, better awareness, improved cyber-policing, and coordinated enforcement is essential to reduce the increasing risk of CNP fraud in India.

**Keywords:** *Card-Not-Present (CNP) fraud, digital transactions, online payment fraud, phishing attacks, SIM-swap fraud, cybercrime in India, banking security, financial cyber fraud, cyber policing, fraud prevention mechanisms.*

[1] LL.M. Student, Department OfHuman Rights, The Tamil Nadu Dr. Ambedkar Law University (SOEL).

[2] Assistant Professor OfLaw, Department Of Criminal Law And Criminal Justice Administration, The Tamil Nadu Dr. Ambedkar Law University, Chennai.

## I. INTRODUCTION

As India moves rapidly towards a cashless and digitally driven economy, the dependence on card-based and online payment systems has increased significantly. The growth of e-commerce platforms, mobile banking applications, digital wallets, and contactless payment methods has transformed the way financial transactions are carried out. While these technological advancements have enhanced convenience, speed, and accessibility, they have also given rise to new forms of financial crime. One such emerging and increasingly prevalent form is Card-Not-Present (CNP) fraud, which has become a major concern for consumers, financial institutions, and regulatory authorities.

Card-Not-Present fraud refers to unauthorized transactions carried out without the physical presence of the payment card. Such transactions typically occur through online shopping portals, mobile applications, telephonic orders, or digital subscription services. In these cases, the offender does not require the actual card but merely needs access to sensitive card details such as the card number, expiry date, CVV, or one-time password (OTP). Due to the absence of face-to-face verification, CNP transactions inherently carry a higher risk when compared to traditional card-present transactions, making them more vulnerable to misuse and fraud.

Several interrelated factors have contributed to the rise of CNP fraud in India. These include large-scale data breaches, weak cybersecurity practices, poor digital awareness among consumers, and the rapid adoption of online services without adequate safeguards. Fraudsters commonly employ sophisticated techniques such as phishing, SIM-swap attacks, skimming, social engineering, and mobile malware to obtain confidential financial information. With increasing access to digital platforms, even individuals with limited technical knowledge have become potential targets of such frauds, thereby expanding the scope and impact of CNP-related offences.

Despite continuous efforts by banks and payment intermediaries to introduce enhanced security mechanisms such as two-factor authentication, transaction alerts, and real-time monitoring systems, fraudsters continue to adapt to evolving technologies. The dynamic nature of cybercrime makes detection and prevention challenging, particularly when transactions involve multiple intermediaries or cross-border elements. The anonymity of digital transactions further complicates investigation and enforcement, allowing offenders to exploit jurisdictional and technological gaps.

The expansion of cross-border e-commerce, international payment gateways, and digital subscription models has further widened the exposure to CNP fraud. From the perspective of economic and cybercrime, such fraud not only affects individual victims by causing financial loss and emotional distress but also undermines public confidence in digital banking systems. Additionally, it imposes significant financial and reputational liabilities on banks and financial institutions, ultimately affecting the stability of the digital economy.

In this context, a comprehensive understanding of Card-Not-Present fraud is essential. Examining its nature, methods, causes, and impact provides valuable insight into the challenges faced by the digital financial ecosystem. This study aims to analyse CNP fraud as a growing form of financial cybercrime in India and highlights the need for stronger preventive mechanisms, increased consumer awareness, and coordinated institutional responses to address this evolving threat.

## I. RESEARCH GAP:

Most available studies on online financial crimes discuss digital fraud in a general way, but very few focus specifically on Card-Not-Present (CNP) fraud in the Indian context. Many papers either explain technical fraud detection systems or describe legal provisions separately, but they do not combine both angles together. Because of these gaps, there is a need for a study that brings together the techniques used in CNP fraud, recent trends and legal responses. This paper attempts to fill that gap.

## II. UNDERSTANDING CARD-NOT-PRESENT (CNP) FRAUD:

CNP fraud is a subtype of debit and credit card fraud that occurs when the cardholder's information is misused without the physical card[3]. It is fundamentally a remote fraud, often conducted through websites, e-commerce platforms, international payment gateways, and mobile payment applications.

It is defined as a transaction is considered a CNP transaction when the merchant does not physically verify the card. Only card details are entered manually for authentication. Hence, any unauthorized use of these details constitutes Card Not Present fraud.

[3] Razorpay, *Card-Not-Present (CNP) Transactions Explained*, 11 Nov. 2025, https://razorpay.com/blog/card-not-present-transactions-cnp/

**Key Characteristics:**

1. **No physical interaction with card or cardholder**

   In CNP fraud, the criminal never touches the physical debit/credit card. They only use the card number, expiry date, CVV, OTP, or other digital details. Because there is no face-to-face verification, it becomes easy for fraudsters to misuse the information.

2. **Often involves data theft or social engineering**

   To perform CNP fraud, criminals usually steal card details through methods like phishing messages, fake websites, fake customer care calls, malware, and data leaks from companies

3. **Cross-border in nature**

   Many times, the fraud is done from another state or country. Because it is done online, criminals can operate from anywhere in the world, making tracking and legal action more difficult.

4. **Difficult for victims to detect immediately**

   Since the fraud happens online without any physical presence, victims often don't realize it immediately. They usually notice only when they got a bank message or while checking the balance.

5. **Difficult for banks to attribute liability**

   Banks face high liability, because the fraud happens without the physical card, banks should need to investigate and compensate the customer according to RBI guidelines. This increases financial risk and responsibility for banks.

## III. Major Techniques Used in CNP Fraud:

1. **Phishing and Smishing**

   Phishing and Smishing are the most common entry points for CNP fraud. In phishing, fraudsters send fake emails and in smishing they send deceptive SMS messages that look like they are from a bank, courier company or government service. These messages contain links that lead to fraudulent websites designed to collect sensitive information. When the victim clicks the link and enters their card details or OTP the scammer immediately gains access. This technique works because the messages appear urgent and legitimate, prompting users to act quickly without verifying.

2. **Database Breaches**

Database breaches occur when hackers break into the server systems of online merchants, payment service providers or even third-party vendors. These databases often store customer information such as card numbers, names, address and sometimes encrypted or unencrypted financial data. Once attackers obtain this information, it is sold on dark web marketplaces or used directly to commit card not present fraud. Database breaches are dangerous because thousands of card details can be leaked at once, increasing the scale of financial loss.

3. **SIM Swap Fraud**

SIM swap fraud involves duplicating the victim's mobile SIM card. The fraudster convinces the telecom operator to issue a new SIM by pretending to the legitimate customer. Once the duplicate SIM is activated, the victim's original sim stops working. The fraudster starts receiving all SMS alerts, including OTPs for inline transactions. This gives them complete control to authorize payments without the victim's knowledge. SIM swap attacks are particularly harmful because even strong authentication becomes useless when the fraudster controls the victim's OTP.

4. **Malicious Apps and Malware**

Fraudsters also use malicious mobile applications or malware-infected software to gain access to banking information. These apps appear harmless, such as free games, loan apps or utility tools but secretly record keystrokes, screen activity or app data. Once installed they silently collect login credentials, card numbers and OTPs. Malware can also redirect users to fake banking pages, making theft easier. Because these apps run in the background, victims usually remain unaware until unauthorized transactions occur.

5. **Credential Stuffing**

Credential stuffing is a technique where fraudsters use stolen email-password combinations from previous data leaks and try them on multiple platforms. Many users reuse the same password across different websites. When fraudsters find matching login, they access accounts containing stored card details or saved payment information. With access to these accounts, scammers make online purchases without needing to know the actual card. This method worked because users often fail to change or update their passwords regularly.

### 6. Man-in-the-Middle Attacks

In man-in-the-middle attacks, scammers intercept communication between the user and the legitimate website during an online transaction. They position themselves in the middle of the exchange by exploiting unsecured Wi-Fi networks or compromised websites. As the victim enters sensitive details, the attacker quietly captures them without disrupting the session. This method is hard to detect because the transaction appears to be happening normally from the user's perspective.

## IV. Why CNP Fraud Is Hard to Detect:

### 1. Transactions appear legitimate

Card-Not-Present (CNP) fraud is difficult to detect because the transactions usually look completely normal in the banking system. Since the fraudster enters all the required details correctly such as card number, expiry date, and CVV the transaction passes through the system as if it was done by the real cardholder. There are no physical red flags like a mismatched signature or suspicious behaviour at a store. As a result, banks and merchants rarely notice anything abnormal at the time of payment. Only after the cardholder checks their statement do they realise that something is wrong, making early detection almost impossible.

### 2. OTP and CVV may already be compromised

In many cases, fraudsters succeed in obtaining the OTP or CVV even before the transaction takes place, which gives them full access to complete online purchases. They do this through phishing messages, fake customer-care calls, or malware that reads sensitive information from a user's device. Once these details are stolen, the security layer becomes useless because the system assumes that the correct person is entering the information. Since the OTP and CVV are the main authentication tools for online payments in India, their compromise directly leads to successful CNP fraud.

3. **Merchant systems cannot distinguish between customer and fraudster**

   During online transactions, merchants depend entirely on the digital data entered by the user, and they have no way of verifying whether the person typing the details is the actual cardholder or a criminal. E-commerce websites process thousands of transactions every minute, and they rely on automated systems instead of manual verification. As long as the entered information matches the records, the system approves the payment. This gap in verification creates a favourable environment for fraudsters who simply mimic legitimate behaviour, making it extremely difficult for merchants to identify suspicious activity in real time.

4. **Cardholder often realizes the fraud much later**

   Most victims of CNP fraud become aware of the fraudulent activity only after checking their bank statements or receiving alerts for transactions they did not make. People do not regularly monitor their transaction history, especially if the amounts deducted are small, which is a common tactic used by fraudsters to avoid immediate detection. Some victims even assume that the deduction is related to an old purchase or a subscription, causing further delay. By the time the fraud is noticed, the attacker would have already completed multiple transactions, making recovery much harder.

5. **Banks struggle with attribution and investigation**

   Banks often face major challenges when trying to track down the person responsible for a CNP fraud. Since the entire transaction happens online without physical presence, it becomes extremely difficult to identify where the request originated or who exactly initiated it. Fraudsters typically use VPNs, fake IP addresses, and temporary devices to hide their identity. Additionally, banks depend on cooperation from merchants, payment gateways, and law enforcement, which slows down the investigation process. Due to these complexities, many cases remain unresolved, making CNP fraud a persistent threat.

## V. TRENDS AND PATTERNS OF CNP FRAUD IN INDIA:

### 1. Rise of Digital Transactions

After 2016, India saw a dramatic shift toward digital payments because more people started using smartphones, UPI apps and internet banking for everyday transactions. The government's push for cashless payments also encouraged people to rely on online modes instead of cash. As digital platforms became more convenient and widely accessible, the volume of online card payments increased sharply. However, this rapid growth also created new opportunities for financial crimes, especially in the online environment where verifying the identity of users is difficult. As a result, the rise in digital transactions naturally led to a parallel increase in cyber fraud cases, including Card-Not-Present (CNP) fraud[4].

### 2. NCRB Data

Reports from the National Crime Records Bureau (NCRB) indicate that cyber-related financial offences have steadily grown over the last ten years. A major share of these incidents involves misuse of debit and credit card details during online transactions, where criminals make unauthorized payments without physically accessing the card. The data also shows that large metropolitan cities such as Mumbai, Bengaluru, Delhi, Chennai, and Hyderabad remain hotspots for these crimes because of their high population density and heavy digital payment activity. These trends highlight that CNP fraud has become a frequent and concerning form of financial crime in India[5].

### 3. Industry Insights

Experts from the payment industry observe that the nature of CNP fraud has evolved as technology has advanced. Fraudsters today use sophisticated methods such as phishing, SIM-swap attacks and database leaks to steal customer information. Industry analysts also point out that many consumers lack awareness about digital safety practices, which makes them easy targets. Additionally, the speed of online transactions gives banks and merchants very little time to verify suspicious activity

[4] NPCI, *Growth of UPI Transactions in India*, https:/0/0w0ww.npci.org.in/statistics (2024).

[5] National Crime Records Bureau, *Crime in India Report 2023: Chapter 9 – Cyber Crimes* (Govt. of India 2024).

before the payment is completed. These insights show that reducing CNP fraud requires both technological improvements and stronger user awareness.

4. **Recent Indian Case Trends**

Recent trends in India show that CNP fraud has become more organised, with criminals increasingly using leaked card data collected from hacked websites and illegal online markets. Many fraudsters now rely on advanced techniques such as SIM-swap attacks to bypass OTP verification and trick banks' security systems. Another worrying pattern is the rise in fraud among first-time online shoppers and elderly users who may not be fully aware of digital safety practices. These factors together reveal that CNP fraud in India is no longer random but part of well-planned cybercrime networks that operate across multiple states.

5. **Financial Impact**

CNP fraud causes significant financial loss not only to customers but also to merchants and banks. Customers may lose money directly from their accounts, while merchants face chargebacks when fraudulent transactions are reversed. Banks, on the other hand, spend large amounts on investigation, refund processing, and upgrading security systems to prevent future incidents. These repeated losses also reduce consumer confidence in digital payments, which affects the overall growth of the online economy. Thus, the financial impact of CNP fraud goes beyond individual victims and affects the entire digital payment ecosystem.

## VI. LEGAL AND REGULATORY FRAMEWORK:

India addresses CNP fraud through a mixture of cyber laws, banking regulations, and criminal statutes.

1. **Information Technology Act, 2000**

The Information Technology Act, 2000 is the primary law that deals with cyber offences, including the unauthorized use of debit and credit card data in CNP fraud. Under Section 66C[6], the Act punishes identity theft, which includes the dishonest use

[6] 66C. Punishment for identity theft.–Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of

of another person’s password, OTP, card number or any other unique electronic identification. Section 66D[7] specifically addresses cheating by impersonation using computer resources — a provision directly relevant to CNP fraudsters who pretend to be bank officials or use stolen digital credentials to complete online transactions. Furthermore, Section 43[8] imposes liability on anyone who accesses a computer system without permission, extracts data, or causes wrongful loss through digital manipulation, while Section 66[9] converts these actions into criminal offences when done dishonestly. These provisions collectively allow authorities to investigate digital payment fraud, penalise offenders who steal or misuse sensitive card information, and hold intermediaries accountable when negligence contributes to the crime. Thus, the IT Act plays a crucial role in India’s legal response to Card-Not-Present fraud within the digital ecosystem.

2. **The Bharatiya Nyaya Sanhita (BNS), 2023**

The Bharatiya Nyaya Sanhita (BNS), 2023 provides the current legal basis for offences involving cheating and unauthorised use of card or online payment credentials in India. Under BNS Section 318[10], a person who fraudulently or dishonestly deceives another and thereby induces them to deliver property, or to do or omit something which causes harm or risk of harm, is punishable by imprisonment up to three years (or fine), while in more aggravated cases where the deceiver is in a position of legal duty toward the victim or induces delivery of valuable securities, the term may extend up to five or seven years. Further, BNS Section 319[11] deals with cheating by personation, and prescribes imprisonment of up to five years in standard

either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

[7] Section 66D. Punishment for cheating by personation by using computer resource.–Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees

[8] Section 43. Penalty and compensationfor damage to computer, computer system, etc

[9] Section 66. Computer related offences.–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both

[10]Section 318 “Cheating”: Describes fraudulently or dishonestly deceiving another person and causing them to deliver property, etc

[11]Section 319 “Cheating by personation”: Offence of impersonation to cheat

cases. By including these updated sections in your paper, you align the legal framework with current law rather than relying on the older IPC provisions.

3. **RBI Regulations**

The Reserve Bank of India has introduced several regulations to strengthen digital payment security and prevent CNP fraud. Key measures include mandatory two-factor authentication, tokenization of card numbers, and strict reporting rules for banks whenever unauthorized transactions occur. RBI also requires banks to establish customer grievance redressal mechanisms and follow timelines for resolving fraud complaints. These regulations ensure uniform safety standards across banks and payment platforms, making them an essential part of India's defence against CNP fraud.

4. **Consumer Protection Act**[12]

The Consumer Protection Act helps victims of CNP fraud by ensuring that banks and merchants follow fair practices and do not place an unreasonable burden on customers. Many consumer commissions have ruled that banks must refund amounts deducted due to unauthorized transactions unless they can prove customer negligence. This framework empowers consumers to challenge unfair refusals and seek compensation under the RBI Ombudsman Scheme. Thus, the Act strengthens the rights of customers affected by fraudulent digital transactions.

5. **Role of NPCI**[13]

The National Payments Corporation of India (NPCI) plays a central role in safeguarding India's digital payment ecosystem. It oversees the functioning of UPI, RuPay and other digital platforms, and ensures compliance with security standards that reduce the risk of unauthorized transactions. NPCI regularly monitors fraud patterns, issues safety guidelines to banks, and updates verification protocols in

[12] Consumer Protection Act, 2019, No. 35 of 2019.

[13] National Payments Corporation of India, *Fraud Monitoring Reports & Guidelines 2024* .

response to new threats. Through these measures, NPCI helps maintain a secure and trustworthy digital payment infrastructure.

6. **Gaps in Enforcement**

   General Payment Framework (GPF) enforcement aims to improve coordination between banks and law enforcement agencies when dealing with digital fraud. However, challenges still exist, especially when transactions involve cross-border networks or foreign websites. Many police units lack trained cyber specialists, making it difficult to trace digital footprints and identify offenders. As a result, investigation timelines are often slow, which affects the overall effectiveness of enforcement efforts.

## VII. CHALLENGES IN DETECTION AND PROSECUTION:

1. **Technical Challenges**

   Technical challenges arise because many fraud detection systems cannot analyse suspicious card activity in real time. Banks may rely on older verification tools that fail to detect advanced techniques used by fraudsters, such as masking IP addresses or using bot-based attacks. Additionally, the involvement of international payment gateways complicates tracking because data may be stored on foreign servers. These technical limitations make early detection difficult and allow CNP fraud to continue undetected for longer periods.

2. **Consumer-Related Issues**

   Technical challenges arise because many fraud detection systems cannot analyse suspicious card activity in real time. Banks may rely on older verification tools that fail to detect advanced techniques used by fraudsters, such as masking IP addresses or using bot-based attacks. Additionally, the involvement of international payment gateways complicates tracking because data may be stored on foreign servers. These technical limitations make early detection difficult and allow CNP fraud to continue undetected for longer periods.

3. **Banking Sector Challenges**

Banks struggle to verify whether a disputed transaction was genuinely unauthorized or resulted from customer negligence. Chargeback processes are often slow because banks must follow strict documentation procedures before approving refunds. They also face difficulties in tracking fraudsters who use anonymous accounts or foreign servers to hide their identity. These issues increase the operational burden on banks and complicate the overall response to CNP fraud.

### 4. Law Enforcement Challenges

Law enforcement agencies face several obstacles when investigating CNP fraud cases. High volumes of daily digital transactions make it hard to identify fraudulent activity quickly, and collecting electronic evidence from foreign websites requires cooperation between multiple jurisdictions. Many police stations lack specialised cyber units, causing delays and reducing the accuracy of investigations. These factors create gaps in enforcement and make it challenging to bring offenders to justice.

## VIII. Key Findings:

The research shows that CNP fraud is increasing faster than many other forms of digital financial crime in India. Most cases arise from unauthorized online card payments, data leaks, and phishing activities that target unsuspecting consumers. Banks have introduced several safeguards, but fraudsters continue to find new ways to bypass verification systems. Enforcement efforts exist, yet the investigation process remains slow and complex, making timely justice difficult.

## IX. SUGGESTIONS:

### 1. Stronger Authentication Technologies

The research shows that CNP fraud is increasing faster than many other forms of digital financial crime in India. Most cases arise from unauthorized online card payments, data leaks, and phishing activities that target unsuspecting consumers. Banks have introduced several safeguards, but fraudsters continue to find new ways to bypass verification systems. Enforcement efforts exist, yet the investigation process remains slow and complex, making timely justice difficult.

2. **Consumer Awareness Campaigns**

A major reason for the rise in CNP fraud is that many consumers are unaware of digital safety practices, making them easy targets for phishing calls, fake links, and social engineering. Regular awareness campaigns through banks, government portals, and social media can educate people about how fraudsters operate and how to protect sensitive information. Mandatory training modules—similar to cyber hygiene classes—can also help first-time digital users understand risks before they begin using online payments. Better public awareness can reduce the number of successful scams and empower customers to identify threats early.

3. **Stricter Merchant Security Standards**

Merchants also play a crucial role in preventing CNP fraud because many frauds occur when criminals exploit weak security systems on e-commerce platforms. All merchants should follow strict PCI-DSS compliance, which ensures that card details are stored, transmitted, and processed securely. Regular security audits, encryption standards, and fraud monitoring tools must be mandatory for online businesses. When merchants improve their cybersecurity practices, it reduces data leaks and prevents stolen card information from entering the hands of cybercriminals.

4. **Improved Cyber Policing Infrastructure**

India needs a stronger cyber-policing network to keep pace with the rapid rise in digital transactions. Establishing digital forensic units in every district can help police analyse electronic evidence quickly and accurately. Dedicated cyber cells with well-trained officers can speed up investigations and improve coordination with banks and payment systems. Better infrastructure ensures that cases do not get delayed due to lack of expertise or resources, and it increases the chances of identifying offenders even when they operate across different states or countries.

5. **Automatic Fraud Alerts**

Introducing AI-based fraud detection systems can help banks identify suspicious transactions instantly. Real-time fraud alerts can notify consumers immediately when unusual activity is detected, allowing them to block the card before further damage occurs. Automated systems can track patterns like sudden high-value purchases, foreign IP addresses, or repeated attempts to enter card details. This proactive approach not only prevents financial loss but also builds trust among digital users by giving them a sense of security.

6. **Faster Refund Mechanisms**

Customers often face long delays and complicated procedures when seeking refunds for unauthorized transactions, which adds to their distress. Banks should introduce clear and simplified refund timelines so that victims are compensated quickly. Provisional credit—where money is temporarily refunded during investigation—can help reduce customer stress and financial disruption. Faster refund mechanisms ensure fairness to victims and encourage more people to report frauds promptly instead of ignoring them out of frustration.

7. **Cross-border Cooperation**

Many CNP fraud networks operate from outside India, using foreign websites, international servers, and global cyber forums to carry out illegal activities. Strengthening cross-border cooperation through MLATs, cybercrime treaties, and international information-sharing mechanisms can help Indian agencies track these criminals more effectively. When law enforcement agencies across countries work together, tracing digital footprints and shutting down fraud networks becomes easier. This cooperation is essential because modern fraud is highly global in nature.

## X. Conclusion:

CNP fraud is a dynamic and rapidly evolving form of economic crime that poses significant risks to India’s digital economy. While technological advancement has made financial transactions easier, it has also widened opportunities for sophisticated offenders. A combination of robust legal enforcement, improved technological safeguards, and informed consumer behavior is essential to reduce the incidence of CNP fraud. As India continues to expand its digital footprint, proactive measures are crucial to ensuring financial security and maintaining trust in electronic payment systems.

## Bibliography

1. Information Technology Act, 2000.
2. The Bharatiya Nyaya Sanhita (BNS), 2023
3. Consumer Protection Act, 2019.

**Websites Referred :**

4. Reserve Bank of India (RBI) – Official Website. https://www.rbi.org.in/
5. National Crime Records Bureau (NCRB) – Crime in India Reports.
6. National Payments Corporation of India (NPCI) – Guidelines & Circulars.
7. Investopedia – “Card-Not-Present Fraud.” https://www.investopedia.com/terms/c/cardnotpresent-fraud.asp
8. Unit21 – Fraud Dictionary: “Card-Not-Present Fraud.” https://www.unit21.ai/fraud-aml-dictionary/card-not-present
9. JATIT Research Journal – “A Proposed Behavioural Profiling Framework for Card-Not-Present (CNP) Fraud Detection.” https://jatit.org/volumes/Vol103No5/23Vol103No5.pdf
10. CERT-In, Government of India – Cyber Safety Guidelines.
11. Press Information Bureau (PIB) – Digital fraud and cybercrime updates.