THE SILENT HEIST: AN ANALYTICAL STUDY OF E-BANKING FRAUDS IN THE INDIAN FINANCIAL SYSTEM

Dr. Ujwala Bendale, Associate Professor, Bharati Vidyapeeth (Deemed to be) University, New Law College, Pune, Maharashtra.

Adv. Vidit Kumar Kanaujia, LLM, Bharati Vidyapeeth (Deemed to be) University, New Law College, Pune, Maharashtra.

ABSTRACT

Broadening the banking services in India has transformed the scenario of financial risk, resulting into an enlargement, more readily available and convenient consequences. Reportedly, in recent years, there has been a dramatic and pronounced rise in the rate of prevalence of channel fraud, The most notable rise being on the internet and using cards. Even when authorities began to focus on safeguarding consumers, enhancing cybersecurity, and keeping an eye on fraud, this occurred.[1]

Recently, there have been allegations of cyber fraud in India, and seems to con artists, who have begun to cash on the emergence of online financial services, mobile banking, and fast payments. deficiencies in technological aspects. They also use emotions such as trust, fear, imitability and hastes.[2]

This article looks at online banking fraud in India, considering the legal and institutional perspective of this issue. It argues that the root cause of the livelihood of digital fraud is an imbalance. Although blocking fraud requires human resource, a payment system incorporates the process to be easy and fast. The essay considers e-banking fraud to be a governance problem as well as a criminal problem. It includes protection of consumers, payments design, cyber law, and those pertaining to the banking sector.[3]

Keywords: E-banking fraud, digital banking risk, cyber fraud, payment systems regulation, consumer protection, cybersecurity governance, financial risk management, India.

[1] Reserve Bank of India, Annual Report 2023-24.
[2] Press Information Bureau, "Curbing Cyber Frauds in Digital India," 30 April 2025
[3] Banking Transactions," 6 July 2017

INTRODUCTION

Among the most striking changes that have been observed over the past few years has been the move to digital banking in India. alterations with the narrative of the financial situation in the country. Introduced convenient payment systems such as online banking, mobile banking, and Unified Payments Interface, have facilitated financial transactions to become easier and faster to everyone.[4] But along with this new infrastructure comes more opportunities to lure victim(s), their accounts and the bank itself, to lose money. Instead of engaging in direct intrusion, the contemporary-day con man always ends up in deception.

A victim can be duped into the disclosure of sensitive data or the authorization of a money transfer by sending them a text message that is presented to look like a bank notification, a fake customer service number, some remote access software, an inappropriate Know Your Customer (KYC) update request, or a false payment collection request.[5] The crime in such or these instances is committed using behavioral methods though the use of technology facilitates the crime.

This situation gives a lot of credence to the idea of the "silent heist." In contrast to the old-fashioned larceny, digital banking fraud is often undetected during the time it is being executed. This discussion explores the intricacies of this phenomenon in the Indian financial system as well as doubts whether the existing legal and regulatory frameworks are sufficiently ready to address it.[6] In most cases the financial loss is not realised until later by which time the funds may have gone through various accounts including intermediary (mule) accounts making recovery efforts more tricky and evidence trails less hard.

SCOPE AND METHODS

An analytical and doctrinal approach is used in this work. It is not merely an effort to list the fraudulent methods. It will examine the role of legal structures, institutional patterns and market reactions in promoting vulnerability and resultant reactions.[7] It makes use of the Reserve Bank of India circulars and annual disclosures, semi-legal provisions enumerated by the Information

[4] Reserve Bank of India, regulatory and supervisory commentary on customer protection and cybersecurity priorities.
[5] Public and legal commentary on cybercrime, phishing, and identity theft in digital finance.
[6] Reserve Bank of India and related reporting on mule accounts, cyber risk, and fraud monitoring priorities.
[7] Reserve Bank of India, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," 6 July 2017

Technology Act, government reports on cyber fraud, and modern analyses of risks incurred in digital payments.

The only electronic banking fraud being examined is those that have impacted the Indian financial ecosystem. All types of online and mobile banking fraud, credit card fraud, UPI fraud, breach of digital identity, fraudulent or unauthorised electronic money transfer are all referred to in this term in the interest of this discussion. Unless they help shed light on the larger financial fraud environment, instances of corporate accounting mismanagement and large-scale loan frauds are not going to be the main focus.[8]

MEANING AND NATURE OF E-BANKING FRAUD

Any bad faith activity where somebody otherwise illegally acquires money, credentials, access, or financial benefits with the help of electronic banking methods or other related digital systems is referred to as e-banking fraud. The term encompasses a wide range of fraudulent activities, such as stealing money from accounts, impersonating someone, using card-not-present transactions inappropriately, phishing, spoofing, mobile app scams, transfers based on impersonation, and misleading requests to accept payments.[9]

The hybrid nature of modern e-banking fraud is different to the previous types of bank-related criminality. There are three different variables to this issue, including cybercrime, fraud and systems design. To defraud another, he might be willing to misuse computer resources, but the last minute bad decision is the last, and it is generally what makes the difference.[10]

This tendency in behavior has become crucial in the situation with digital payments in India. Despite the minimization of transactions to a few seconds, due to mobile-first payment systems, fraud prevention remains necessary to detect, assess, and sometimes communicate between institutions. The organisational disparity is stark, having seconds to coax a victim, to freeze cash in their wallet might require an array of organisations and may take a long time.[11]

[8] Reserve Bank of India, Annual Report 2023-24.
[9] India Code, Information Technology Act, 2000, section 66D.
[10] Policy discussion on securing digital payments and calibrating friction in digital transactions.
[11] https://economictimes.com/news/economy/policy/rbi-red-flags-increased-risk-of-cyber-attacks-digital-frauds-and-data-breaches/amp_articleshow/116689247.cms

TYPOLOGIES OF FRAUD IN INDIAN E-BANKING

Phishing and spoofing

Phishing is one of the frequent varieties of attacks even in the realm of online banking. Through spoofing, the identity of the sender or the receiver is concealed making the message or phone call appear more authentic. The idea would be to deceive the victims so that they share sensitive data with us, such as, a login id or One-Time Password (OTP), by making it look like the communication might have been made by an institution that they trust.[12] The legal issue associated with these strategies are at the intersection of pretenses and illegal entry. Under Indian cyber regulations there are repercussions of phishing attempts that result in identity theft, illegal password use, or fraud through impersonation using computer resources.[13]

Identity Theft and Impersonation

Considering its appearance, identity theft has become even more significant, becoming an essential part of the financial crime performed over the Internet. The Information Technology Act specifically deals with identity scams and impersonation using computer resources and this indicates that law makers realise the possibilities of computer based identities misuse.[14] As a matter of fact, by changing or counterfeiting identities, one may find it easier to evade verification checks, activate mobile connections, open accounts, run mule accounts or to deceive counterparties when engaging in financial transactions.[15]

Even fictional bank executives have been unable to get out of impersonation. Today cybercriminals are very good at deceiving individuals into believing they are legitimate business, government and even friends and acquaintances on social media and other messaging web sites. Due to its versatility, digital fraud is not merely a financial challenge, but an ecosystem one, where the false creation of trust signals in many platforms is also a part.[16]

UPI and Instant-Payment Fraud

Fraud involving the Unified Payments Interface (UPI) warrants some special consideration

[12] Public and legal commentary on cybercrime, phishing, and identity theft in digital finance.
[13] Press Information Bureau, "Digital Security of Citizens"
[14] India Code, Information Technology Act, 2000, section 66D
[15] https://finlawassociates.com/blog/identity-theft-punishment-legal-consequences-and-penalties-in-india
[16] Government and public reporting on cyber fraud harms and complaint ecosystems

since it entails the most prominent achievement of India in the field of digital payments. Common tricks used by fraudsters in this sector include exploiting user lack of understanding on how to use QR codes, how to get their money back and what to do when they click collect rather than refund and that a collect request causes a debit authorisation to take place instead of a refund mechanism being invoked.[17] Victims may mistakenly believe that scanning a QR code solely facilitates the receipt of funds, or that a collect request is part of a refund mechanism when, in actuality, it triggers a debit authorization.

The fast nature of UPI increases its vulnerability to fraud and its social benefit. Though business could be served well by a system that emphasizes fast settlement arrangement, it leaves no time to reflect, identify and act. Various measures to restrict dubious transactions in the form of the application of chosen friction, better due diligence, and procedural safeguards have thus taken centre stage in the current legislative discussions over the safety of online payments.[18]

Card and Internet-Banking Fraud

Reportedly associated with the fiscal year 2024 of the Reserve Bank of India (RBI), traditional channels such as card and internet banking are still highly vulnerable to exploitation, per reports.[19] The importance of this is that it demonstrates that the two categories of banking fraud in terms of volume were card and internet fraud.

Cards fraud can take the form of credential compromise, card-not-present transactions, breaches that are involved with skimming, and illegal use of saved payment credentials. This is a lesson that it is not just a single product in digital finance that fraud is pervading the layers.[20] The institutional lesson underscores that fraud evolves to infiltrate every layer of digital finance rather than being confined to a singular product.

STATISTICAL AND REGULATORY PATTERN

In any legal discussion of the problem of e-banking fraud that has any importance whatsoever, it is essential to begin with the trend in this area. Although this may not necessarily imply that

[17] Press Information Bureau, “Digital Security of Citizens”
[18] Policy discussion on securing digital payments and calibrating friction in digital transactions
[19] Reporting on FY24 card and internet fraud patterns in Indian banking
[20] Public and legal commentary on cybercrime, phishing, and identity theft in digital finance

there has been a decrease in other forms of frauds being pursued in the daily activities of the fraudsters, it does imply that the primary emphasis of the daily fraud activities by the fraudsters have moved to channel that encounter retailing activities, such as online banking and mobile payments, and that digital-channel frauds, especially card and internet frauds, have risen dramatically and become the most reported fraud cases, according to RBI reporting FY24 and related studies.[21]

Subsequently, reports of Financial fraud in FY25 reflected that a lesser number of incidences had been met. The downward trend has been sharply decreasing, thus we should exercise care on making conclusions.[22] The underreporting or a change in categorisation method or concentrating the lost value among fewer instances of e-banking fraud cannot be resolved merely by a glance at the reported case numbers that may reflect an increased level of control, more ignorance, or even deterrent.

Apparently, e-banking fraud is the overall tendency in cybercrime. It is not whether or not there is a problem of financial victimisation in digital form and increased sophistication of cyber-enabled scams, it is whether or not the institutional response to e-fraud is keeping pace with the growth of digitalisation.[23] Thus the issue is not whether India has a digital fraud problem; the issue is whether the institutional response to e- fraud is keeping pace with the growth of digitalization?

THE LEGAL FRAMEWORK GOVERNING E-BANKING FRAUDS

Information Technology Act, 2000

The relevant act of cyber- law that is relevant to e-banking fraud is the Information Technology Act. Section 66D covers e-banking fraud involving the use of a false name and computer resources, as compared to identity theft in general (Section 66C).[24]

Wherever fraudsters utilise fake digital representation in e-banking to compel transfers, abuse credentials, or impersonate individuals or organisations online, these requirements are immediately involved. It is not so much the criminalisation of e-banking fraud which is of

[21] Reserve Bank of India, Annual Report 2023-24.
[22] ET Government, "Digital Frauds in Banks Halve in FY25 After Previous Year's Surge: RBI Report"
[23] Press Information Bureau, "Curbing Cyber Frauds in Digital India," 30 April 2025
[24] India Code, Information Technology Act, 2000, section 66D

importance to the IT Act, but its classification. It considers that the cognisable ills related to the e-banking fraud are digital identity, electronic access, and computer-mediated deceit. The majority of today's payment frauds do not involve brute-force attacks on systems, but rather digital representation and the fraudulent acquisition of confidence in online banking. This is of the utmost importance.[25]

Criminal law overlap

The doctrinal importance of the relationship between e-banking fraud and laws of deceit, fraud, forgery, criminal conspiracy, dishonest inducement depends on the circumstances surrounding a particular instance of e-banking fraud.[26] Despite the tool possibly being digital, it does not override or eliminate the traditional criminal culpability of e-banking fraud, instead it only adds to it; it does not remove it. Although enforcement agencies have more leeway because to cyber-law and criminal rules coexisting, the lack of standardisation in reporting formats for e-banking fraud might lead to a muddled investigation and classification process. To victims, the distinction means the world more than a theory: the route taken by the complaint will determine when freezing e-banking fraud-funds is possible and what the time frame will be.[27]

RBI's customer-protection framework

The tool that is imperative is Regulation of e-banking fraud: RBI circular on Limiting Liability of Customer in Unauthorized electronic Banking transactions.[28] The circular describes the customer responsibility, zero liability and limited liability all of which are subject to the type of fault and how soon an attack is reported. The framework is portrayed in a just distribution of e-banking frauds.

While acknowledging that in the case of e-banking fraud, and the fraud stays timely reported, the client should not be charged responsible of the damages caused by the flaws in the bank systems or the damage caused by a third party, irrespective of whether the customer was at fault. On the one hand, it presupposes that the reasonable precautions and the responsiveness

[25] https://finlawassociates.com/blog/identity-theft-punishment-legal-consequences-and-penalties-in-india
[26] https://blog.ipleaders.in/punishments-cyber-crimes-ipc/
[27] Press Information Bureau, "Curbing Cyber Frauds in Digital India," 30 April 2025
[28] Reserve Bank of India, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," 6 July 2017

of consumers to avoid the e-banking fraud cases would occur.[29]

Liability, burden and victim protection

The question of responsibility is likely to be the most controversial question which appears after an event of e-banking fraud. Bankers assert that customers caused the loss since they provided their OTPs, tapped links, or engaged in any other actions. The problem is that it is frequent that the security measures of the bank are not adequate or fail to comprehend the activity and the customers often complain about the fact that security measures of the bank were inadequate or failed to understand the activity.[30]

Only by following the regulations set by the RBI, both banks and clients will have the laws regulating responsibility become effective. Unless both banks and customers are aware of who they need to report to, then it may take a long time before the customers receive help whether there are regulations in place to protect the customers.[31] The reason is that a system that restricts who can work best when customers are informed and can report problems quicker and banks can know whether a customer made an error, was deceived or if the system has failed. We do not just want regulations regarding repayment as a measure to protect those already victims of scam. We should inform them immediately, enable them to make any complaints feasible and, within the bounds of law, certainly stay any dubious transactions. More likely, the money will be saved should the bank or any other organization start responding faster to the problem.[32]

INSTITUTIONAL AND SYSTEMIC VULNERABILITIES

The human factor

A widespread misconception is the belief that the problem of digital fraud is only technical. To defraud banks, scammers do not necessarily have to be experts in codes; many scams in e-banking take advantage of peoples trust in authority, fear of blockage of their account, a quick fix is needed, confusion over interface with payment.[33] They should simply have the capability of being able to communicate to others. This emphasises the need of educating consumers

[29] Mondaq, commentary on RBI's customer-liability circular
[30] Reserve Bank of India, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," 6 July 2017
[31] Reserve Bank of India, regulatory and supervisory commentary on customer protection and cybersecurity priorities
[32] Reserve Bank of India and related reporting on mule accounts, cyber risk, and fraud monitoring priorities
[33] Public and legal commentary on cybercrime, phishing, and identity theft in digital finance

about security. This education should be interested in the mechanics of transactions instead of the general campaign at the mass media. This is meant to sensitize the users on the red flags of some activities and those things that reputable institutions would never demand.[34]

Mule. Layered movement of funds

Since mule accounts make it difficult to retrieve funds after they have been conned, the RBI has spoken about how they facilitate scams.[35] Mule accounts are significant. When they use accounts created with this in mind, then it becomes even harder to detect and prevent the transfer of funds. The mule-account problem is one instance of a problem with online banking fraud. After a debit has been made, the perpetrator takes off with the victim in pursuit, cashing checks and withdrawing money, and even switching platforms. It is due to this that we do not see the scam in its entirety when we become fixated on the victim and the bank.[36]

Speed versus security

The digital payment system in India is based on quickness, ease, and accessibility. Even more economically advantageous, however, is how much a payment system should slow down in order to prevent fraud, a problematic issue posed by the design itself.[37]

Over-slow down might negate legitimate business and inclusivity. Even a small delay can so that a fraudulent(or otherwise) transaction can be completed prior to any protection becoming effective. Not to skate without a purpose but to smarten skate speed is the better way to act. Additional verification or delay can be required due to the high risk of transactions, the inclusion of odd beneficiaries, or suspicious behavioural patterns.[38]

Analytical findings

Three major conclusions can be made out of this debate. First, contrary to their breaking into systems, people are increasingly being duped in the internet banking fraud in India. That does not make it less of a problem but it does require that organisations should prioritise security

[34] Government and public reporting on cyber fraud harms and complaint ecosystems
[35] https://economictimes.com/news/economy/policy/rbi-red-flags-increased-risk-of-cyber-attacks-digital-frauds-and-data-breaches/amp_articleshow/116689247.cms
[36] Reserve Bank of India and related reporting on mule accounts, cyber risk, and fraud monitoring priorities
[37] Policy discussion on securing digital payments and calibrating friction in digital transactions
[38] https://industrialeconomist.com/rbi-seeks-views-on-securing-digital-payments/

measures in the forms of interface design, structure of warning and customer communication, and identity assurance.[39]

Moreover, the regulatory framework is significant, but it is dynamic. The IT Act, and the customer-protection system of the RBI, can be a source of redress, but is largely ineffective in preventing the problem, rather than resolving the issue afterwards. A post facto solution is less effective than a preventive/delaying solution in high-speed payment situations.[40]

As a third point, the regulatory system is currently giving less attention to it. There has been no change to the fraud ecosystem.[41] The fact that the government has an issue with the mule accounts and cybersecurity and digital-payment integrity suggest that the issue is not going away, and reports of a decline in fraud cases point to the fact that the measures can be effective.[42]

RECOMMENDATIONS

This should be a concerted effort to fight fraud in four major areas in India. To begin with there must be an upgrade to risk-based authentication in a financial institution and payment intermediaries. Sensitive transactions, devices, the introduction of new beneficiaries, and suspicious behavior of a request should trigger additional levels of authentication.[43]

Secondly, there must be more standardised tighter inter-institutional cooperation. To curb loss of funds incurred, speed at which fraud intelligence, signals regarding the risk of the beneficiaries, as well as information about suspected mule accounts should be shared within the ecosystem.[44]

Third, the implementation of consumer protection should be operational instead of having the documentation. Principles to be used when eradicating complaints, recording transactions, requesting temporary freezing and communicating with customers should be in line with

[39] Public and legal commentary on cybercrime, phishing, and identity theft in digital finance
[40] Reserve Bank of India, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," 6 July 2017
[41] ET Government, "Digital Frauds in Banks Halve in FY25 After Previous Year's Surge"
[42] https://economictimes.com/news/economy/policy/rbi-red-flags-increased-risk-of-cyber-attacks-digital-frauds-and-data-breaches/amp_articleshow/116689247.cms
[43] Policy discussion on securing digital payments and calibrating friction in digital transactions
[44] Reserve Bank of India and related reporting on mule accounts, cyber risk, and fraud monitoring priorities

principles used under the liability principles of RBIS.[45]

The fourth aspect is that there must be a new approach in behaviour regulation in the classroom. To avoid the usual scam scripts scams alerts must be pre-programmed to show at various points during the payment process and written in clear English.[46]

CONCLUSION

In India, the e-banking frauds have now become a large regulatory burden, instead of unfortunate byproduct of digital finance.[47] Although there has been a recognition of some of the problems by the legal system, the sheer fact that these scams are ever-increasing in complexity, goes to show that even with this level of awareness, nothing has yet been put in place to help control them in systemic ways.[48]

The main thesis of the present essay is that the e-banking fraud is more successful when time is of a essence and digital trust is easily created as opposed to being verified. A more developed framework for digital finance, rather than a withdrawal from banks, is the way forward. One that considers the interdependence sides of fraud prevention as user behaviour, payment design, institutional coordination and legal accountability.[49]

[45] Reserve Bank of India, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," 6 July 2017
[46] Press Information Bureau, "Curbing Cyber Frauds in Digital India," 30 April 2025
[47] Reserve Bank of India, Annual Report 2023-24.
[48] India Code, Information Technology Act, 2000, section 66D
[49] Policy discussion on securing digital payments and calibrating friction in digital transactions

REFERENCES

1. Reserve Bank of India, Annual Report 2023-24.
2. ET Government, "Digital Frauds in Banks Halve in FY25 After Previous Year's Surge: RBI Report".
3. Reserve Bank of India and related reporting on mule accounts, cyber risk, and fraud monitoring priorities.
4. ET Government, "Digital Frauds in Banks Halve in FY25 After Previous Year's Surge".
5. Reserve Bank of India, regulatory and supervisory commentary on customer protection and cybersecurity priorities.
6. Reserve Bank of India, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," 6 July 2017.
7. Mondaq, commentary on RBI's customer-liability circular.
8. India Code, Information Technology Act, 2000, section 66D.
9. Press Information Bureau, "Digital Security of Citizens".
10. Press Information Bureau, "Curbing Cyber Frauds in Digital India," 30 April 2025.
11. Public and legal commentary on cybercrime, phishing, and identity theft in digital finance.
12. Reporting on FY24 card and internet fraud patterns in Indian banking.
13. Policy discussion on securing digital payments and calibrating friction in digital transactions.
14. Government and public reporting on cyber fraud harms and complaint ecosystems.
15. Commentary on card and internet fraud channels in India's banking environment.