E-BANKING FRAUDS AND SAFETY SOLUTIONS: ANALYSIS

Nikita Johri, Vth year law student at University of Petroleum and Energy Studies, Dehradun

ABSTRACT

This paper proposes to highlight the online banking frauds in India, its statistics, category of security threats related to it, legal provisions regulating the e-banking as well as the guidelines by RBI to control risk due to e-banking. Since, e-banking has become the new trend in the banking sector, it is important to consider the loopholes of this system and frauds which can take place. Further, I will end this paper by suggesting some ways to avoid online banking frauds.

Introduction

An increase in digitalization, supported by technology advancements and the rise of intelligent systems, has caused a paradigm shift in how the banking industry operates. The historically labor-based banking organisations are evolving into an automated versions i.e., conventional banking is evolving into electronic banking. Customers gain from the convenience of 24-hour banking. The banks are now able to provide products and services in real time and greatly reduce the cost of banking. This has lead to the various e-banking frauds as reported by central banks and state governments. Similarly, safety solutions have to be evolved as similar level of fraud is executed through multiple internet banking, mobile banking and Internet payment system (IMPS) frauds. In today's context it has become essential to study the frauds related to E-banking in India. In current scenario, everyone have access to the internet, even though they are not technically sound or professional. With this in mind, many such people have started using e-banking services online in India as well as abroad. One of the biggest benefits of e-banking is that one can do transactions in just a few clicks.

At present there are many factors which may contribute to the increase in the number of frauds related to E-banking. First and foremost among them is that many people still believe that they are secure when they use online banking. Also, there is a lack of awareness among people as well few common threats and methods of conducting fraudulent transactions (as per RBI data).

Frauds in the e-banking sector

Internet banking fraud is a type of theft or fraud that involves the unauthorised withdrawal of funds from one bank account and/or the transfer of funds to another bank account utilising online technology.[1] The following categories[2] best describe *security risks* in a system that uses electronic banking:

- **Disclosure of Login Details**: The most popular method by which criminals obtain login information, such as a number or PIN, required to access anyone's account and steal money.

[1]*Internet banking frauds,* WORLD JUTE.COM http://www.worldjute.com/ebank1.html#:~:text=Internet%20Banking%20Fraud%20is%20a,through%20techniques%20such%20as%20phishing.
[2] Sarala. M S, *E-Banking Frauds and RBI Guidelines,* https://www.inspirajournals.com/uploads/Album/512859974.pdf

- **Computer spyware viruses:** These are computer programmes that spread via email or other methods. Upon opening a malicious email, a customer's computer will immediately download and install a programme. These programmes gather login credentials or other financial data, which is then used to carry out a variety of illegal acts like credit card fraud or illicit money transfers.
- **Dummy sites:** Criminals will occasionally establish dummy websites that closely resemble bank websites. When users enter their login information, this information is captured and used for criminal purposes.
- **Loss of Personal Relationship:** Since e-banking does not involve face-to-face interaction, there is a loss of faith in the operation and the products of e-banking. To make up for this, e-banks must offer high-value products and reduce operating expenses to stay competitive, which may further decrease the opportunities for developing a human connection with consumers.
- **Organizational structures and resistance:** E-banking calls for significant managerial and structural changes in the company. Given that changes are typically not accepted in any business, this could cause morale issues. The success rates of projects that use change management are lower.
- **Ethical Concerns:** In this context, the main ethical concerns might relate to the security and privacy of personal information about individuals, information accuracy, ownership of information and intellectual property, accessibility of information held, and what ethically acceptable uses of this information are. These concern freedom of choice, transparency, and assisting in fraud (other people's unethical or unlawful behaviour).

Types of online banking frauds

Internet banking fraud is a type of identity theft that is frequently made possible by scams like phishing and lottery fraud.[3] In India, the following types of banking fraud are most common:

- **Stolen credit or debit card:** People often find themselves in such situations wherein they lose their debit or credit card, which if found by the person with malafide intentions can cause an immense loss. Which is why it’s best suggested by the banks to get the cards blocked as soon as they go missing.

[3] Rupesh. D. Dubey, *e-banking frauds and fraud risk management,* TACTFUL MANAGEMENT RESEARCH JOURNAL, http://oldtm.lbp.world/SeminarPdf/167.pdf

- **Cloning of debit or credit cards:** As the system grows people find nefarious ways to challenge the system and find new loopholes in order to extort the money by various illegal means and this is one such means in which cloning of debit or credit cards can be easily done.
- **Phishing or fraudulently making customers give their own information:** One of the most common banking frauds is phishing, where scammers try to trick customers into giving them their personal or financial information. Phishing is the act of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
- **Stolen PIN number or banking passwords:** Once the card's personal identification number (PIN) is obtained, PIN cashing typically entails using an ATM to withdraw money. A data breach that occurred during the processing of cards is what led to this type of cybercrime.[4]
- **Hacked accounts and mobile apps:** Even though mobile banking apps are far safer than browsers for accessing financial services, they are still subject to fraud, money laundering, and cyberattacks.

  Inadequate security procedures and technology tripwires may be the cause of many passwords that have been stolen and unauthorised transactions.[5]
- **Stolen CVV and OTP number:** In a typical OTP scam, the con artist calls the victim and pretends to be interested in your good or service. They consent to pay a specific sum right away as confirmation and then ask for information on the payment gateway or digital wallet, followed by the OTP. The fraudster can start a number of transactions to drain your account once they have gained access to it. Many minor frauds frequently go unnoticed.[6]

Legal Framework Regulating E-banking

The financial industry has seen significant changes as a result of globalisation, privatisation, and liberalisation. The switch from branch banking to online banking has made room for new competitors. Traditional banking is under serious threat from the smart system of revolution,

[4] Jake Frankenfield, *Pin Cashing*, INVESTOPEDIA, (February 17, 2021), https://www.investopedia.com/terms/p/pin-cashing.asp
[5] FINEZZA, https://finezza.in/blog/mobile-banking-frauds-prevent/
[6] Hitesh Raj Bhagat, *OTP & digital fraud raising its ugly head. Here is what you should do*, THE TIMES OF INDIA, (September 22, 2021), https://timesofindia.indiatimes.com/blogs/voices/otp-digital-fraud-raising-its-ugly-head-here-is-what-you-should-do/

which is bringing competition and technological progress together. Stringent laws must be passed to control the financial industry. This does not solve the issues, hence more regulations and legislation must be introduced in order to address the issues with e-banking.

The Legal Framework for Banking in India is provided by a set of Enactments, viz.

- The Banking Regulation Act, 1949: Since banking frauds are not directly addressed by the Banking Regulation Act of 1949, one seldom ever considers using this Act's provisions to combat banking frauds. However, the provisions of this Act do assist one comprehend the workings of the banking industry to some extent, which may help one understand the causes of banking frauds.

- The Information Technology Act, 2000: A new class of technology offences, whose prevention is incidental to the maintenance of a secure electronic environment for e-banking and the prevention of banking frauds and forgeries, has also been created by the IT Act 2000, which also amended the Indian Penal Code to include conventional offences committed electronically. A few provisions of the RBI Act of 1934 were also modified by Section 94 of the Act. Some of the ways that financial frauds are committed online include digital forgeries, unauthorised access to computer networks, data manipulation, skimming, online identity theft, and impersonation.

- The Reserve Bank of India Act, 1934: The Reserve Bank of India[7] uses the 1995-introduced Electronic Cleaning Service (ECS) and Electronic Fund Transfer (EFT)[8], as well as the 2004-introduced Real Time Gross Settlement (RTGS) system, 2005-introduced NEFT system, and 2008[9]-introduced check transaction system.
  In addition, the Reserve Bank of India published advice on risk reduction strategies and security concerns related to card present transactions. By requiring banks to provide additional authentication or validation for all-in-one recurring transactions based on information not present on credit, debit, or prepaid cards, the RBI has taken steps to protect card not present transactions.

[7] Under the Reserve Bank Of India Act, 1934, 'Bank' means Reserve Bank of India constituted by this Act.
[8] https://en.wikipedia.org/wiki/Electronic_funds_transfer accessed on 30/10/22 at 3 A.M.
[9] https://www.researchgate.net/publication/279753172_About_legal_framework_of_e-banking on 20/10/22 at 3 A.M.

The legal basis for establishing bank holding corporations was also supplied, and it paved the door for the licencing of new banks. The RBI has been providing commercial banks with numerous guidelines and regulations regarding information technology, electronic banking, technical risk management, and cyber crimes.

- Indian Contract Act, 1872: What constitutes a contract is defined in Section 10 of the Indian Contract Act. There is a contractual arrangement between a banker and the customer, as was already mentioned. Consequently, it may be claimed that the Act will be somewhat applicable in addressing financial frauds in India.
  According to Section 16 of the Act, being under the influence is a form of deception that is somewhat less severe. The idea of fraud is fully covered in Section 17 of the Act, and misrepresentation is covered in Section 18. The notion of constructive fraud was examined by the court in Oriental Bank Corporation v. John Flentming[10]. [11]Section 19 also addresses the voidability of contracts that lack free consent.

- Indian Penal Code, 1860: The Indian Penal Code does not specifically define the term "fraud" or classify financial fraud as a separate offence. However, there are some provisions in the act that are invoked in cases of banking fraud.
  According to the Indian Penal Code, counterfeiting coins[12] or currency notes[13] is an offence and constitutes a case of fraud. Additionally, Chapter XVIII of the Code is reported to contain rules connected to financial frauds, including sections 378[14] and 379[15], which discuss theft and its associated penalties.

Guidelines by RBI to Control Risk Due to E-Banking

Benami Accounts: According to the law, bankers are not allowed to maintain any anonymous

[10] (1879) 3 Bom. 242,287
[11] In this case it was observed that this clause is probably intended to meet all those cases which are called in the court of equity -cases of constructive fraud, in which there is no intension to deceive, but where the circumstances are such as to make the party who derives a benefit from the transaction equally answerable in effect as if he had been actuated by motives of fraud or deceit.
[12] Section 231 of the IPC deals with Counterfeiting coins.
[13] Section 489-A of the IPC deals with Counterfeiting coins of currency notes
[14] Section 378 of the IPC states that whoever intending to take dishonestly any movable property out of the possession of any person without consent, then the person is said to be commit theft.
[15] Section 379 of the IPC states that whoever commits theft shall be punished with imprisonment of either description for a term which may extend to 3 years or fine or both

accounts, accounts in fictitious names, or accounts in the names of people whose identities are kept a secret.[16]

Threshold limit: Banks must pay extra attention to transactions involving big sums of money and unusual transactions. On the basis of customer information, background information, funding sources, and other factors, banks must establish key indicators for these accounts. Accounts of gold and jewellery merchants should be frequently reviewed. Suspicious Transactions Reports (STRs) must be sent on a regular basis to the Financial Intelligence Unit-India (FIN-IND). Once more, a frequent evaluation of risk categorization is required.[17]

Monitoring: Due to the fact that Multi-Level Marketing businesses work with public funds and guarantee increased earnings, their finances need to be routinely checked. When banks notice any odd activity, such as a high number of checks with the same dates and amounts, they should notify the RBI and FIN-IND of the problem.[18]

Parameters for Risk Perception

Based on the type of business activity, the location of the customer and his clients, the method of payment, and the customer's societal standing, customers should be divided into low, medium, and high risk categories.

KYC Adherence: The internal audit should be knowledgeable about KYC guidelines and protocols. They should review the KYC practises used in the branches and address any shortcomings they find. Additionally, this must be reported on a quarterly basis to the board's audit committee.

Pay Particular Attention to Money Laundering Threats: Banks give a range of cards to customers who help with financial activities. Typically, this is accomplished with the aid of agents. Therefore, before issuing such cards, bankers should make sure that the proper KYC procedures are correctly applied. And these safeguards should apply to the agents as well.

[16] Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on May 10, 2021, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11566&Mode=0

[17] Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002, https://m.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=6520

[18] Adherence to KYC/AML guidelines while opening and conduct of the accounts of Multi Level Marketing firms, https://rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=5271

Maintenance of Information: Bans must keep records of referred transactions that allow for the reconstruction of individual transactions. These records must include the following information: the nature of the transaction, the type of currency used, the amount transacted, the date of the transaction, and the parties involved.

FIN-IND: Banks are required to notify the Financial Intelligence Unit of India if they have any suspicions regarding a transaction or if they are asked to disclose account details for a customer.[19]

Statistics of online banking frauds

According to information provided to the Rajya Sabha, cases of online fraud decreased by around 17.5% in FY22, from 160 crore to 128 crore, as compared to the previous fiscal's record of 160 crore. A thorough approach has been devised to combat online banking fraud.

“As per RBI data on frauds reported by Scheduled Commercial Banks (SCBs) under the category “Card/Internet- ATM/Debit Cards, Credit Cards and Internet Banking", the amount involved in such frauds, based on the year of occurrence, has declined from Rs. 185 crore in the financial year 2019-20 to Rs. 160 crore in the financial year 2020-21 {year-on-year (Y-o-Y) decline of 15.2%} and to Rs. 128 crore in the financial year 2021-22 (Y-o-Y decline of 17.5%),"Minister of State for Finance said in the Lok Sabha.

"RBI has issued instructions on Cyber Security Framework in Banks and have mandated SCBs to report all unusual cyber incidents to RBI within two to six hours of occurrence of such incidents. These incidents are analysed for the pattern of attack and the vulnerabilities exploited, and where needed, advisories/alerts are issued to the banks so as to avoid repeat attacks/exploitation of the same vulnerabilities,: the Minister informed the House.

The corrective steps taken by the Government to prevent fraud and cheating through online transactions[20]

1. A comprehensive circular on Cyber Security Framework in Banks was issued by RBI on 2.6.2016, wherein banks were advised to put in place a board-approved cyber-

[19] PMLA, 2002 – Obligation of Banks, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=4188

[20] Govt shares data on online banking fraud and how many cases solved, MINT, https://www.livemint.com/news/india/govt-shares-data-on-online-banking-fraud-and-how-many-cases-solved-11660007363092.html

security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk.

2. Guidelines on Cyber Security Controls for third party ATM Switch Application Service Providers (ASPs) have been issued by RBI on 31.12.2019.
3. Master Directions on Digital Payment Security Controls have been issued by RBI on 18.2.2021, wherein banks have been advised to put in place necessary controls to protect the confidentiality and integrity of customer data, and processes associated with the digital product/services offered.
4. A National Cyber Crime Reporting Portal has been launched by the Ministry of Home Affairs to enable public to report incidents pertaining to all types of cybercrimes, and a toll-free number has also been operationalised to get assistance in lodging online complaints.
5. For immediate reporting of financial frauds and to stop siphoning-off of funds by the fraudsters, Financial Cyber Fraud Reporting and Management System module has been made operational by the Indian Cyber Crime Coordination Centre (I4C), working under the Ministry of Home Affairs.
6. The Indian Computer Emergency Response Team (CERT-IN) under the Ministry of Electronics and Information Technology issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies, and is working in coordination with service providers, regulators and LEAs to track and disable phishing websites and facilitate investigation of fraudulent activities.

How to avoid e-banking frauds in India?

The Reserve Bank of India has issued certain guidelines[21] for users in case they fall victim to online banking frauds:

1. Banks must create their banking system and procedures in order to make way for safe net banking for customers.
2. The liability of customers is limited in case of any unauthorised net banking transactions.

[21] Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11040

3. The banks must inform their customers about SMS and email alerts for online banking transactions.
4. If an unauthorised online transaction has taken place because of a third party and it is reported within 3 days by the customer, the bank must credit the amount back in the customer's account within 10 days of receiving the complaint.
5. If a customer delays in reporting an online banking fraud within 3 days and delays for 4-7 days, the customer will be penalised with up to Rs. 25,000 fine depending upon the type of bank account, credit card held by the customer and any gift cards used.
6. The liability for delay in reporting online banking fraud for Basic Savings Bank Deposit (BSBD) account is Rs. 5000; the liability for delay in reporting online banking fraud for Savings account, prepaid transactions, an overdraft account, Current account, cash credit account, gift cards accounts for MSMEs and accounts for individuals with an annual balance or limit of Rs. 25 lakhs, is Rs. 10,000; for other accounts with credit card limit of Rs. 5 lakhs, the maximum liability is Rs. 25,000.
7. For the loss caused by an unauthorised transaction, the bank will be held liable.
8. For unauthorised transactions with third party liability, any delay in reporting will attract liability up to the amount of transaction.
9. For a delay beyond 7 days, the customer liability will be determined in accordance with the bank's policy approved by the Board.
10. The banks must resolve the customer complaint within 90 days of receiving it.[22]

Suggestions

In light of the discussion of the subject above, the following recommendations can be made:

- Education campaigns on the use of e-banking services and products must be regularly organised.
- Age, occupation, and gender-based customization of e-banking services.
- To maintain computer security, banking employees should also include technological specialists.
- Making investments in the security and privacy of client data.
- To make the rural population literate, special awareness campaigns must be launched.

[22] https://www.myadvo.in/blog/online-banking-fraud-in-india/ on 30/10/22 at 4 A.M.

- Additionally, the government needs to implement strict measures for defaulters.

Conclusion

E-banking is still in its infancy in India. The banks are making the necessary steps to incorporate new technology into their services and products to benefit the public, but there is still a long way to go. Banks promote their services through advertising so that people are aware of new plans and policies without any difficulty. The younger generation is adjusting to it, and the majority of their e-banking job is completed promptly via online banking. E-banking evolved into a popular banking method throughout time. E-banking offers pertinent, appropriate information while saving time and money.

Banking frauds are a typical occurrence in the modern world. The general public places its savings in banks not just for the meagre interest rates that offer but also for reasons of security, but whenever bank frauds take place, the public loses faith in banks. Nowadays, scarcely a day goes by without news articles reporting on bank fraud and forgery events. These frauds might include theft, robbery, debit card and credit card fraud, as well as frauds performed online, particularly when internet banking is involved.

There are definitely laws in place that aid us in preventing banking frauds in some way. Ironically, though, there is no special legislation that addresses fraud and forgery in the financial industry. Indian financial frauds are always understood and prevented by referring to the Indian Penal Code, 1860. The Indian Penal Code does not specifically define the term "fraud" or classify "banking fraud" as a separate offence.

References

Dr. Roshan Lal, Dr. Rajni Salluja, E-Banking: The Indian Scenario,

www.indianresearchjournals.com.

M.L.Tannan, Tannan's, Banking Law and Practice in India, (20th Ed.), (New Delhi:

India Law House, 2003), p.157

R.N.Chaudhary, Banking Laws, and (1st Ed.), (New Delhi: Central Law Publications,

2009). p.377.

https://www.myadvo.in/blog/online-banking-fraud-in-india/