Online Banking Fraud in India

Dr. Kumudha Rathna,
Department of Business Law,
The Tamil Nadu Dr. Ambedkar Law University.

Introduction

In this 21st century our daily life dwells with the technology, we want everything to be done instantly, our expeditious approach towards every aspect of our life made changes in the way we approach everything in our daily life. As we can see there is tremendous growth in every sector including banking service, we opt for online banking instead of traditional banking system which needed our physical presence for every service. Whereas online banking can be done wherever we are, and the transaction can be done within few minutes and its available for 24*7. As the growth in banking sector help us with swift service, it also carries the risk of online banking frauds. It makes consumer lose money within few seconds, most of them unaware of possible risk in online banking. Online banking still did not reach its perfection; thus, we must be aware of the possible risk of using the new technology for our comfort.

What Is Online Banking

Online Banking is the method in which transactions are made through internet with the help of electronic devices such as computers, smartphones, table, etc., Banking sector provide consumer the secured and speedy banking service via internet, as banking system growing towards the process of enhancing their system with the usage of IT, more expected data protection methods and measure to secure consumers can be achieved. But even after such security measure consumers still lose money in online banking frauds making us question where the fault lies.

Online banking frauds

Online banking frauds is nothing but illegally obtaining bank credentials to steal consumers money without their knowledge. In some instance by other fraudulent means such as phishing, cloning of debit/credit cards, using lost credit/ debit card, etc, As we can see online banking crimes are interlinked with the cybercrime. In some instance we may not know whether the culprit is the bank itself, mainly if the bank fails to take due diligence to maintain proper details of all the customers. The failure of banks due diligence in not maintaining the KYC database will lead to not availability of transaction details of the receiving customer, which leads incline in online banking frauds. There are several instances where the bank is the defaulter for the loss of innocent bank account holder. As we all know there is rising use of internet banking by Indians, the number of online banking frauds in India has increased significantly. Let's have a look at the types of frauds and preventive measures that can be taken.

Types of Online Banking Frauds and Issues [1]

SIM Swap Fraud

Juice Jacking/Hacking:

When his iPhone vibrated in his pants pocket, **AMIT Kumar Mishra** was in Central Delhi's Connaught Place for a reunion. It wasn't an SMS message. On the screen, a 'low battery' warning had appeared. The 39-year-old inserted his phone into a free USB power charging station that was nearby.

The party was about to be ruined when he received a notification that Rs. 50,000 had been deducted from his bank account, despite the fact that he had made no such transaction.

Cops told that there are several cables in the market where hackers get access to all the texts, messages, emails, photos, contacts etc. This is majorly done at shopping complexes and airports to steal bank details

This hacking is termed as JUICE JACKING. Hackers use a USB charging cord to carry out a Juice Jacking attack. When a user plugs his charging cable into his phone's charging port and connects it to one of the rigged charging stations situated in public places like airports, railway stations, hotels, and cafés, hackers get access to the affected device through the back door. The charging connector, which is also utilized for data transfer via USB, has been identified as the primary source of concern. Installing malware, wiping user data, demanding ransom for access to personal data on the phone, and hijacking personal and financial accounts are just a few of the evil things a hacker may do with this unlimited access.

Vishing:

A vishing attack is a type of fraud in which thieves call a potential victim and pose as a corporation, attempting to persuade them to provide personal information.

Legislative Framework:

The Payment and Settlement System Act 2007[2]

It is a law that regulates and governs Payment Gateways in India, with the goal of ensuring that all payment and settlement systems operating in India are safe, sound, efficient, and appropriately secured, among other things. The Reserve Bank of India is given authority under this act to supervise and manage all payment and settlement systems in India, as well as to guarantee settlement finality and a clear legal basis for them.

[1] https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf

[2] The Payment and Settlement Systems Act, 2007|Legislative Department | Ministry of Law and Justice | GoI

The Indian Contract Act of 1872

It defines what constitutes a contract in Section 10 of the Act. A contractual relationship exists between a banker and a consumer, as previously stated. As a result, the Act would be relevant in dealing with banking frauds in India to some extent.
Section 16 of the Act refers to being under the influence, which can be classified as a lesser degree of deception.
Section 17 of the Act elaborates on the idea of fraud
Section 18 addresses misrepresentation. The court examined the idea of constructive fraud in **Oriental Bank Corporation v. John Flentming,** this case was well-known for contract misrepresentation, in which one party did not examine the content of the terms of agreement and was harmed by the other party's deception, and brought a lawsuit against him. This case is significant for the section 18 of the Indian Contract Act of 1872.

Legal Remedies for internet banking fraud

Information Technology Act of 2000[3]

The first step is to notify the bank as soon as possible. The bank must take reasonable steps to guarantee that its customers have access to secure online banking. The bank must install CCTV cameras in its offices and ATMs, warn consumers of any transactions from their accounts via email and SMS alerts, track irregular or unexpected transactions, and so on.

A person who is a victim of online banking fraud can file a complaint with the Adjudicating Officer under Section 46 of the Information Technology Act, 2000, alleging that the bank failed to implement appropriate security measures. Banks and other intermediaries that do not adopt acceptable security measures for safe banking are required to provide adequate compensation to customers, according to Section 43A of the Information Technology Act of 2000. The bank must demonstrate that it took adequate steps to prevent any illegal or unauthorized transactions.

RBI Ombudsman Scheme:

If the bank fails to take action after submission of the complaint regarding deficiency of service, the consumer can lodge complaint against the bank based on RBI Ombudsman Scheme, whereas before approaching the ombudsman, the consumer must file the complaint with the bank. Only after bank fails to respond within 30 days from the lodgement of the complaint or if the bank rejects the complaint wholly or partially the consumer can approach the Ombudsman. The RBI Ombudsman Complaint can be made through the online portal at https://cms.rbi.org.in/cms/indexpage.html#eng[4]

[3] A2000-21_0.pdf (legislative.gov.in)
[4] Reserve Bank of India - Complaints (rbi.org.in)

Cyber Cell:

For Online transactions frauds, it is important to lodge a complaint in cyber cell in the nearest area, if cyber cell is not available the complainant can lodge a complaint in the nearest Police Station explaining the complete incidence about the unauthorized transaction and loss of money by unknown person. While lodging complaint it is important to collect 6 months bank statement of the concern bank, to make a copy of SMSs received related to the alleged transaction, to take ID proof and address proof as shown in the bank records. Further, complain can be lodged through cybercrime online portal at https://www.cybercrime.gov.in/Default.aspx[5]

Possible suggestions to reduce bank frauds:

There are a number of ways to protect yourself from these types of cyber-attacks which includes:

1. Keep track of all SMS/Emails- While conducting business, it is a good idea to check all messages, pops, and other types of texts.
2. Only transact with reputable and certified online merchants- Buying products from reputable and marketplaces is highly recommended. Payments are safe when made through well-known e-commerce sites. However, before purchasing anything, it is recommended that you read their terms and conditions.
3. Never share confidential information- According to Phone Pay, you should never share confidential information such as your credit/debit card number, CVV number, or OTP (One Time Password) with anyone, even if they pose as an official representative from the bank or a third-party mobile app. Instead, tell them to send the information to your official email address registered with the bank.
4. Antivirus, firewall, and other security software should be installed on all computers and devices. It is also recommended to avoid charging laptops or smartphones in public locations and to use HTTP websites.
5. Use public charging outlets cautiously. These are easy targets for hackers since they are frequently left unprotected and unmonitored. Even if you're using them, verify the USB ports' power source behind the charging station.

Conclusion

Daily news clearly shows the amount of struggle the general public go through in life while dealing with online transaction, even though the technology advancement in banking sector helps old age people and those who reside in abroad to take care of their loved once without hurdles, it is significant to mention the need for enhancement and development to protect the innocent bank account holders. As we can see clearly from the RBI notification which explains about the Zero liability of the consumer and the recent judgement by the apex court and Consumer forum emphasising more responsibility on the bank to prove the consumers default and to take appropriate measures to revert bank the unauthorised transaction made by the unknown person and also by providing adequate compensation for the losses suffered by the innocent consumers. In some instance court insist that the bank should not collect any money from the customer if the transaction is clearly marked as a "disputed transaction" and thus shows the evolvement

[5] Cyber Crime Portal (www.cybercrime.gov.in/Default.aspx)

in our legal system and the adequate measures taken by the courts and forum to safeguard consumers as far as possible.

References

1. https://legislative.gov.in/sites/default/files/A1986-68_0.pdf
2. A2000-21_0.pdf (legislative.gov.in)
3. The Payment and Settlement Systems Act, 2007|Legislative Department | Ministry of Law and Justice | GoI
4. Reserve Bank of India - Notifications (rbi.org.in)
5. INGRAM | Integrated Grievance Redressal Mechanism (consumerhelpline.gov.in)
6. Reserve Bank of India - Complaints (rbi.org.in)
7. Cyber Crime Portal
8. Cyber Cell warns of rampant KYC fraud as more people lose money in Coimbatore - The Hindu
9. Arupukottai man loses ₹59,000 in online fraud - The Hindu