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

VOLUME 4 AND ISSUE 4 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

ECONOMIC CRIME – ONLINE BANKING FRAUD & ITS TYPES

AUTHORS – K. SHIVASANKARI* & MS. T. VAISHALI**, LLM SCHOLAR* & FACULTY OF LAW** AT SCHOOL OF EXCELLENCE IN LAW, TNDALU

BEST CITATION – K. SHIVASANKARI & MS. T. VAISHALI, ECONOMIC CRIME – ONLINE BANKING FRAUD & ITS TYPES, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (4) OF 2024, PG. 827-831, APIS – 3920 – 0001 & ISSN – 2583-2344.

ABSTRACT:

Banking Industry has undergone digital disruptions at a massive level. Online booking, mobile apps, and E-bill payments have become the norm. People are mostly occupied by the internet, computer, and mobile phones nowadays. Banking transactions are digitized from back end to front end, and digital transactions are made without any human intervention. This study has been undertaken to analyze online banking frauds such as phishing, smishing, card fraud, etc., and also the causes behind it. And giving the preventive measures to the people to safeguard from Online bank fraud in India. Online banking, while offering unparalleled convenience, has also become a prime target for cybercriminals. This paper delves into the multifaceted landscape of online banking frauds, examining their various types and the sophisticated techniques employed by perpetrators. We discuss the most prevalent methods, including phishing, vishing, smishing, malware attacks, and social engineering. Additionally, the paper explores the financial and psychological implications of these frauds on victims, highlighting the need for robust security measures. By understanding the intricacies of online banking frauds, individuals and financial institutions can adopt proactive strategies to mitigate risks and safeguard sensitive information. Online banking fraud is a rapidly growing problem in the digital age. It occurs when criminals gain unauthorized access to an individual's online bank account and transfer funds without their knowledge or consent.

KEY WORDS: *Banking fraud, digital transaction, scams*

INTRODUCTION:

Online Banking Fraud or Internet fraud refers to schemes in which fraud is committed by a criminals because of poverty, poverty is about not having enough money to meet basic needs including food, clothing and shelter so they are committing this fraud .In this fraud they are illegally obtaining bank credentials to steal consumers Money without their knowledge and this Online banking frauds involve cybercriminals exploiting vulnerabilities in digital banking systems to steal money or sensitive information. Online banking frauds are also called digital banking fraud. 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.[1265]Online banking fraud refers to the unauthorized use of online banking services to commit fraudulent transactions, steal sensitive information, or disrupt banking operations.

MEANING AND OBJECTIVES OF BANKING FRAUD:

Online banking fraud is a rapidly growing problem in the digital age. It occurs when criminals gain unauthorized access to an individual's online bank account and transfer funds without their knowledge or consent.It is an illegal act of an individual person obtaining money, assets, or other property from a

[1265] https://www.futurelearn.com/info/courses/fraud-investigation-making-a-difference/0/steps/65530 20.11.24 [4] https://www.bankofbaroda.in/banking-mantra/digital/articles/common-internet-banking-frauds-and-preventiontips 20.11.24

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

financial institution. Bank fraud is becoming more prevalent and can cause significant financial and reputational damage[4]. Bank fraud is a major problem for financial institutions and can have a serious impact on their customers and its main objectives is to prevent online banking fraud by implementing robust security measures, such as two factors authentication, encryption and secure login protocols and to know about the norms of the Reserve Bank of India related to online banking. To detect online banking fraud in real- time, Using advanced technologies, such as machine learning and Artificial intelligence and to analyze steps taken by banks in preventing online banking frauds and how to provide precautionary measures to the public for online banking fraud.

TYPES OF BANKING FRAUD:

"Phishing" means cyber criminals sending emails or text messages containing action links. Clicking the link leads to a fake webpage designed to access personal information[5]. In this type, fraudsters may call people and ask them to renew their bank account or credit card. Phishing scams are mostly done through SMS and e- mail directed to a link[6] through such fraud, scammers send clickbait messages that resemble official bank messages. "Gift fraud" or Advance-fee fraud occurs when people pay money online expecting loans, lottery prizes, or gifts. Example: Fraudsters may impersonate customs officers asking for fees for clearance but ultimately victims lose money. In "Fake loan fraud" the fraudsters will randomly call numbers from the data of prospective person. In this they will call person who is looking for loan and they will use a phishing technique later to collect money. In "Fake apps" Counterfeit banking apps deceive users into providing personal information[7] fake apps are malicious application created by cybercriminals to steal personal information [8]Example: Fake G pay or Pay tm apps. In "card skimming" fraudsters will record the information of people's payment cards like debit and credit cards for fraudulent transaction. "Vishing attack" is a type of fraud in which thieves call a potential victim and pose a corporation, attempting to persuade them to provide personal information. Website spoofing is building a fake website to commit fraud is called website spoofing. But Phishers use the names, logos , pictures and website codes to make spoof sites appear authentic. While using the website after checking the presence of 'HTTPS' in the URL can enter the details.[9] "Malware and spyware" fraudsters will use malicious software to infect victim's computer or mobile devices. This malware can capture keystrokes, screen activity, and personal information and spyware is malicious software that enters a user's computer ,gathers data from the device and users, and it will sends to third parties without their consent [10] In Fake Bank website", the fraudulent websites replicate bank sites to trick users into entering login credentials. Fake Bank websites are malicious websites that mimic the information appearance and functionality of legitimate bank websites. These websites are designed to trick users into. providing sensitive information, such as login credentials, credit card number and Personal Identification Numbers (PINs)[1266] criminals create fake Bank websites to mislead and entice people into transferring money or disclosing personal information.[12]

"Session hijacking" is a type of cyber-attack where an attacker takes control of user's session, allowing them to access sensitive information and perform actions as if they were the legitimate users. Hackers intercept and will take control of online banking session. Criminals steal personal information to access and control bank accounts. To prevent session hijacking, website owners need to use HTTPS across their entire website and strengthen session management [1267]"Identity theft" in online

[1266] https://www.aubank.in/blogs/8-different-types-of-digital-banking-frauds 20.11.24

[12] https://www.fdic.gov/consumer-resource-center/2023-10/scammers-and-fake-banks#:~:text=Criminals%20create%20fake%20bank%20websites,a%20false%20sense%20of%20security. 21.11.24

[1267] https://www.keepersecurity.com/blog/2024/04/03/what-is-the-best-way-to-prevent-session-

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

VOLUME 4 AND ISSUE 4 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

banking fraud refers to the unauthorized use of a person's sensitive information, such as their name, address, date of birth, and financial details, to commit online banking fraud[1268]. In fraud through investment schemes Involve using funds from new Investor to pay off earlier investors, promising unrealistic high returns. In "UPI fraud", in this fraud scammer sends Money to victims account through a UPI apps and they will contact the victim requesting for a payback. If he repays through UPI app means then malware inflects their device, giving the fraudster access to their full data including bank and KYC details. In "online banking transaction fraud", Unauthorized transactions are made using stolen card information or account credentials. This type of fraud can result in financial losses for individuals, businesses and financial institutions. In "SIM SWAP scam" scammer just issues a new sim card on the customer's current registered mobile number thus receiving all the alerts and OTP's requires to easily perform any banking transaction from the customer's bank account.[1269]

PRECAUTION:

Use strong and unique password to avoid using easily guessable information such as your name, birthdate or common words and enable Two Factor Authentication (2FA) this adds an extra layer of security to your online banking account. Should keep your operating system and browser up to date to ensure to have the latest security patches and updates installed and Avoid attending calls from unknown numbers asking for sensitive details and ensure that your online banking platform is secure and reputable and avoid using a public Wi-Fi on unsecure network to access your online banking account regularly check your account statements and transaction history to detect any suspicious activity be wary of emails and messages that ask you to provide sensitive information or click on suspicious links And report to bank immediately . Verify website URLs and ensure they start with 'https'. People should not disclose their OTP and PIN number with any other persons. Use Anti- virus software and keep it updated. Share security best practices with family and friends.

CASE LAWS AND INCIDENTS RELATED TO ONLINE BANKING FRAUD:

Some incidents related to Online banking Fraud includes:

1) "SBI Phishing Scam (2011)": SBI customers received fake emails and texts asking for login credentials. Hackers stole ₹1.5 crores from affected accounts .so they told to verify website authenticity be cautious with links.

2) "SBI Malware Attack (2010)": SBI customers devices were infected with malware and in this hacker had stolen ₹1.5 crores. So, they advised to keep antivirus software updated and use secure networks.

3) "ICICI Bank Phishing Scam (2007)": In this case ICICI Bank customers received fake emails asking for login credentials. Hackers had stolen Rs.2.5 crore from affected accounts.

So, beware of phishing emails, verify sender authenticity.

Some cases related to online Banking Fraud include:

1) ***Sujit Menon vs State of Maharashtra (2019):*** The Bombay High court ruled that Phishing attacks fall under *Section 66D of the Information Technology Act, 2000* which deals with punishment for cheating by impersonation using computer resources[1270]

hijacking/#:~:text=Session%20hijacking%20is%20a%20cyber,gain%20access%20to%20their%20account. 21.11.24

[1268] https://www.eset.com/in/identity-theft/#:~:text=Identity%20Theft-,Identity%20theft%20is%20a%20crime%20in%20which%20an%20attacker%20uses,by%20their%20own%20econo mic%20gain. 21.11.24

[1269] https://us.norton.com/blog/mobile/sim-swap-fraud#:~:text=SIM%20swapping%20happens%20when%20scammers,'%20device%2C%20not%20your%20smartph one. 21.11.24

[1270] Sujit Menon vs State of Maharashtra (2019)

2) ***ICICI Bank Ltd. vs Abhijeet Bhattacharya (2018):*** The Delhi High Court held that banks must compensate customers for online fraud unless they can prove gross negligence on the customers part the customer must be compensated for unauthorized transaction.[1271]

3) ***State of Kerala vs N. Sivakumar (2017):*** The Kerala High Court ruled that online banking fraud falls under *Sections 420 (cheating) and 406 (criminal breach of trust) of the IPC* and they said that IPC provisions apply to online transaction also[1272]

4) ***Mrs. Sucheta Charudatta Dhekane vs Bank Of Maharashtra (2011):*** This case established the bank's responsibility to protect customers from internet banking frauds and phishing activities. The court held the bank liable for losses incurred by the customer due to fraudulent transactions, emphasizing the bank's duty to implement robust security measures.[1273]

SUGGESTIONS:

Online banking fraud poses a significant threat to individuals and organizations alike. To mitigate this risk, it's essential to implement robust preventive measures. A multi-layered approach is necessary to safeguard against online banking fraud. Firstly, strong and unique passwords are crucial for online banking accounts. Additionally, enabling two-factor authentication adds an extra layer of security Regular software updates are also vital to ensure that operating systems, browsers, and antivirus software have the latest security patches. Moreover, being cautious of phishing scams is essential, as these scams can trick individuals into revealing sensitive information To further protect against online banking fraud, using a secure internet connection, reputable antivirus software, and a firewall is recommended. Using a secure browser and logging out securely also helps prevent unauthorized access In the event of suspected online banking fraud, swift action necessary. Contacting the bank immediately and filing a police report can help minimize damage. Furthermore, monitoring credit reports and considering a credit freeze can help prevent further unauthorized activity. Ultimately, a proactive approach to online banking security is crucial in today's digital landscape. By implementing robust preventive measures and staying vigilant, individuals and organizations can significantly reduce the risk of online banking fraud.

CONCLUSION:

Online banking fraud poses a significant threat to individuals, businesses, and financial institutions. A multifaceted approach is necessary to safeguard financial transactions. The diverse array of fraudulent tactics exploited by cybercriminals. This includes proactive security measures, customer education and awareness, and enhanced collaboration between financial institutions and law enforcement Online banking fraud presents a significant challenge in the digital age. While technology offers unparalleled convenience, it also creates opportunities for cybercriminals to exploit vulnerabilities. To effectively combat this threat, a multi-faceted approach is necessary. Financial institutions must invest in robust security measures, including advanced fraud detection systems, strong encryption protocols, and robust authentication processes. Additionally, raising awareness among users about online security best practices is crucial. This includes educating individuals about the dangers of phishing attacks, the importance of strong passwords, and the need to be vigilant when conducting online transactions. By fostering a culture of cyber-awareness and implementing stringent security measures, we can effectively mitigate the risks associated with online banking fraud and safeguard our digital financial lives.

[1271] ICICI Bank Ltd. Vs Abhijeet Bhattacharya (2018)
[1272] State of Kerala vs N. Sivakumar (2017)
[1273] Mrs.Sucheta Charudatta Dhekane vs Bank Of Maharashtra on 9 November, 2011