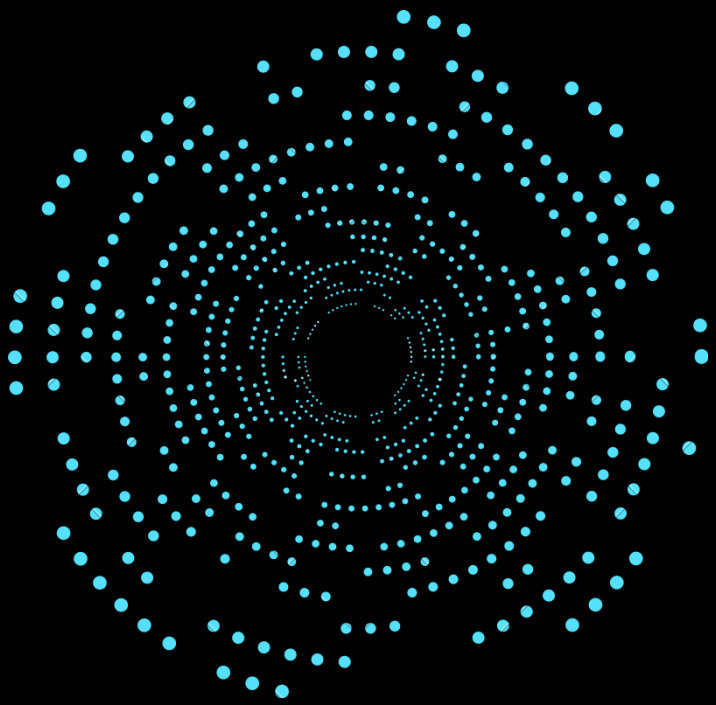
INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY



VOLUME 1 AND ISSUE 1 OF 2023

INSTITUTE OF LEGAL EDUCATION

International Journal on Cyberspace Law and Policy

(Free Publication and Open Access Journal)

Journal's Home Page – https://ijclp.iledu.in/

Journal's Editorial Page - https://ijclp.iledu.in/editorial-board/

Volume 1 and Issue 1 (Access Full Issue on - https://ijclp.iledu.in/category/volume-1-and-issue-1-of-2023/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

Volume I and Issue I of 2023

ISBN - 978-81-960677-4-8

Published by

Institute of Legal Education

https://iledu.in

FINANCIAL CRIMES IN CYBERSPACE

Author - PRACHI SHUKLA, STUDENT AT S. S. KHANNA GIRL'S DEGREE COLLEGE, UNIVERSITY OF ALLAHABAD

Best Citation - PRACHI SHUKLA, FINANCIAL CRIMES IN CYBERSPACE, *International Journal on Cyberspace Law and Policy,* 1 (1) of 2023, Pg. 75-81, ISBN - 978-81-960677-4-8.

ABSTRACT

With the advancement of information and communication technology (ICT) the world has gradually stepped-in to a wholly virtual space called- "cyberspace". The global communication and easily accessible information is a bane as well as a boon for mankind. That is to say, on one hand the ICT is cementing the path of technological development on national and international level and on the other hand the hi-tech networks and evolving technology has made individuals vulnerable to a lot of wrongful or malicious acts in the cyberspace which is commonly known as cybercrime. To begin with the list of cybercrimes there are many categories but the most popular among those several categories in the recent decades is- cybercrime in financial activities/ the financial crimes in cyberspace. For transactions individuals as well as the banking sector have shifted largely to online banking platforms and transactions through mobile phones, e-banking, debit/ credit card, etc. The expansion of ICT in areas of banking and finance is indeed much useful in the fulfilment of day-to-day requirements of individuals and business institutions. But on the very next step it poses grave threats to the user's personal information and details which the individual would otherwise keep as confidential, like:- individual's bank account details, credit card information, ATM pin, account password, etc. Also, cybercrime in finance occurs due to lack of awareness among individuals, wherein even pin-point negligence can land them as victims in the hands of cybercriminals. This article aims to identify the most frequent forms of financial cybercrimes, scanning the redressal available in case of cybercrimes in finance in Indian context.

KEY WORDS:- Cyberspace, finance, cybercrimes, banking fraud, I4C scheme**.**

Introduction

A strong banking sector is the spine of any developing economy. The growth of this sector is indeed an inevitable pre-condition for healthy and steady development of the national economic sector. In 21st century the development of banks has led to an increase in the practice of money transactions physically as well as through online and electronic medium like:- debit/ credit card, ATM card, UPI, Google Pay, Paytm, etc., which undoubtedly proves to be feasible for the users/ individuals and owing to which there is diversification of activities in the banking and financial institutions. But with the growing edges of technology the cyber frauds or cyber hackers are always ready to grab you tight in their web so that you lose all your sensitive, confidential

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

and utmost important data and information in the hand of such fraudsters and become the victim of cyber fraud or cybercrime. Same is the case with online financial transactions and transactions which anywhere involves together- money, internet and any electronic device (laptop, mobile phone, etc.) which we generally refer to as "financial cybercrime".

The services that have been created for the convenience of individuals/ users/ customers are generally misused by the cyber criminals, which lead to financial frauds in the cyberspace. The cyber frauds/ cybercrimes in finance occur when the criminals of cyberspace use hacking and social engineering techniques together for the purpose of financial gain. Thus, it will not be wrong to say that the economic crimes that are being committed in the virtual space are committed by the exploiting the social-engineering and hacking techniques that easily make their way through the security systems of the financial and banking institutions. The cyberspace offers worldwide access to each and every person alongwith the benefit of keeping one's identity anonymous over such a wide area of network (cyberspace). Consequently, the perpetrator of the cybercrime in financial activities often remains unidentified.

Financial crimes in cyberspace refer to the illegal act of digging out crucial, sensitive information or data wrongfully with the motive of wrongful economic gain. Basically, it is a criminal activity for the purpose of wrongful financial gain. This involves phishing, vishing, ransomware attacks, email and KYC frauds, theft or attempt of theft of confidential bank account information/ other payment card information, denial of service attacks, etc. There is still a need of wholesome knowledge awareness and attitude of alertness in the environment of cybercrime in the context of finance and allied activities with regard to cyber hackers and their advancing social-engineering techniques.

I. Types of Financial Cybercrimes

:- The various categories of cybercrime in financial activities include:-

(A) Security Hacking:- The act of gaining unauthorized access to an individual's computer or networks with intention and for the purpose of obtaining an individual's personal data and information and then exploiting that information for their personal benefits, is known as hacking. The hackers can break in to an individual's as well as an instituion's/ organization's computer system and networks depending on their need. Gaining wrongful access to a computer system or even attempting to breach the security build-up of any banking/ finance institution or an individual/ company's account or confidential payment card details by hacking is also a financial cybercrime.

(B) Identity Theft:- When a person say- X, gains access into a computer system or any other electronic device of any other person in order to collect that other person's personal and private information, and then uses that information falsely to create alike identity of himself as that of the other person in order to access the bank accounts of that other person, his credit card information, making purchases through his payment card options, and other unauthorized transactions.

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

(C) Spyware:- The most common method of stealing the financial or banking credentials of an individual/ company/ organization and then making their use for the purpose of illegal transactions is "spyware". It is a kind of malicious software which after its installation begins to access the device on which it is installed without the knowledge of user of the device. It functions by transmitting, gathering and exporting information of the user from his device across other devices and networks. Basically, the purpose of this software is to steal OTPs, banking credentials, sensitive passwords and credit card numbers.

(D) Cyber Laundering:- Cybercrime and money-laundering are the two essential elements which when combined constitute cyber laundering. Actually, cyber laundering refers to the process of making use of internet in order to launder the illicit amount of money so that it seems to be clean and is generally non-traceable. Cyber laundering exploits the internet and other digital platforms for the purpose of transferring and concealing funds that have been obtained illegally. Cyber laundering makes use of much complex and advanced technologies, in order to render the illegal transferability of funds arising from illegal activities non-traceable and anonymous, thus making it the sophisticated type of money-laundering. Cyber laundering is mostly done through virtual currencies or through the use of encryption techniques and tools. It allows the criminals to hide and exploit the proceeds which they have obtained from their illegal acts.

(E) Cryptojacking:- Cryptojacking refers to the unauthorized use of someone's mobile device or computer resource wherein it embeds itself within any of the respective devices and thereafter makes use of the device's resources to mine cryptocurrency. Cryptography unlike other types of cybercrimes in finance does not depend on stealing the victim's data, rather it uses the resources of the victim's mobile or personal computers in order to render free money to the hijacker/ the attacker without incurring huge expenses on paying electricity bills (due to establishment of huge computer networks for the lawful mining of cryptocurrency). These hackers (cryptojackers) employ the computing ability of their victim's device to solve the complex problems and earn the cryptocurrency. A device after being cryptojacked, the cryptojacking functions in the background of the victim's device without victim having the knowledge of the same, thereby resulting in excess battery usage, lag in the device's performance, or even high computing bills.

(F) Phishing:- An email or a general message often pops-up on our devices like computers or mobile phones that flaunts before us the urgency of updating the username, or passwords, or credit card credentials, or such other information related to our personal financial outreach for which it contains a malicious attachment or a malicious

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

link and requires the individual to click on that link or attachment and most importantly the fact that it seems to have been sent by a legitimate source or on behalf of a legitimate authority. The criminal intent behind sending such scam emails is to bait the user to open the attachment or click on the malicious links and as soon as the user does so all his confidential sensitive information such as passwords or login credentials or credit card information goes in the hands of those cyber criminals.

(G) Vishing:- Voice and phishing when combined together constitute vishing. In vishing criminals veil themselves as banking officials or other authorized or legitimate personnel over a phone call, or a mechanized audio message with an intention to dig out the confidential and sensitive details regarding the user's bank account, username, OTP, credit card expiry date, ATM pin, etc. Such phone calls generally state some issue with the individual's bank account or require reactivation of his ATM card or ask for the credit card/ ATM card details in such a manner that the individual/ user as soon as possible involves himself in the process, thereby leading to the flow of sensitive information about the user's bank account or ATM card details or any other essential financial details to the fraudster. The mechanized audio messages also function similarly, often by motivating the user/ individual to claim the prize money.

(H) Ransomware:- It is a type of malware which is utilized by attackers/ the cyber criminals to hold their victims hostage in context of their data, in return of a payment/ fee. An attack like ransomware begins with phishing mails (generally carrying malicious attachments). As soon as the user opens the malicious attachment his device gets infected by malware, and that malware then scans the files in order to encrypt the files and lock them. Other attacks happen through drive by downloading when the user visits an infected website, which downloads the malware without the user having the knowledge[108].

(I) Pharming:- In this form of attack the user/ the customer logging in or trying to reach a particular bank's website is directed or routed to some other spam website that is not legitimate but seems to be real like the original website. Thus, such false website has the potential to extract all the important sensitive and confidential data regarding that user's financial details and use them for wrongful purposes and for the benefit of such cyber criminals[109].

II. How Cyber Security Can Be Applied In Financial Institutions Like Banks

:- Below is the list of some of the most important cyber security tools. These are:-

(A) Software Security:- Software security provides protection to those applications or software that are crucial for the operations

[108]."What are the types of Cyber Attacks on Financial Institutions?", https://www.fortinet.com/solutions/industries/financial-services/types-of-cyberattacks-on-financial-institutions.
[109] Himanshi Lodha, Divya Mehta, "An Overview of Cybercrimes In Baking Sector", https://www.legalserviceindia.com/legal/article-7694-an-overview-of-cyber-crimes-in-banking-sector.html.

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

of business. Software permits listing and signing the code and has characteristics like an application which could assist us in synchronization of our security policies alongwith permissions for sharing files and few other authentication factors. Artificial Intelligence (AI) is definitely going to be the game changer in software security.

(B) Safeguarding Sensitive Systems:- Attack on huge systems can only be avoided with the establishment of broad area network. Wide-area network strongly hold the strict standards of protection, to follow, which the industry has set for its customers or users in order to safeguard their connections and devices. It keeps a check on all programs of the institutions being performed and also a check on network and users for the purpose of safety and security of the institution as well as the users.

(C) Risk Management:- Risk management essentially serves the cause of evaluating the risk and then taking the preventive action to prevent the possible harm or the expected loss. Cyber security involves within it the concept of risk management and for the purpose of risk management factors like- analysing the risk, data integrity, and data security training play a crucial role.

(D) Surveillance of Network Security:- The term 'surveillance' refers to constantly monitor something to put a check on the cons or the negative impact of something. Surveillance of network security refers to constantly scanning the network against any sort of phishy, malicious or intrusive activity. This network security surveillance can be done either manually or automatically. The network security surveillance is performed alongwith anti-virus software, and firewalls.

III. Solutions/ Remedies Available In India In Situations Of Financial Cybercrime

:- The ever shooting rise in transactions through online mode has resulted in a significant increase in financial crimes in cyberspace. The Reserve Bank of India (RBI) also has acknowledged the problem of cyber frauds in finance and thus, introduced a Master Circular in July 2016 i.e., "Master directions on Fraud-Classification and Reporting by Commercial Banks and select FIs".

I4C Scheme**:-** The Government of India, seeking to handle the problem of ever increasing financial crimes in cyberspace, launched the I4C scheme in 2019 i.e., "Indian Cyber Crime Coordination Centre" under the supervision of Ministry of Home Affairs. Several units like- National Cybercrime Reporting, National Cybercrime Forensic Laboratory (NCFL), National Cybercrime Research and Innovation Centre, National Cybercrime Threat Analytics Unit, etc. were set up for the purpose of identifying and investigating cybercrime. In the instances of financial crime being committed in cyberspace the victim can inform about/ report about the happening by lodging a formal complaint on the National Cyber Crime Reporting Portal or by making a call on 1930. In the instances of financial cyber fraud the victim has to access the portal (National Cybercrime Reporting Portal) and register him/ her as a user. After registering as a user the victim is required to select "Report Cybercrime" and then select the name of state where the complaint has to be lodged. Thereafter, the complaint, according to circular of RBI on frauds i.e.,

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

'Frauds: Classification and Reporting', is forwarded to the cyber cell and then FIR is lodged at the police station of the state where the offence is allegedly committed[110].

There is not a single law that specifically deals with financial frauds in cyberspace. In such instances, as according to the circulars of RBI at the time of registration of such cases provisions of the Indian Penal Code would be invoked. "Time" is the most crucial essence of any cybercrime and as per the I4C scheme the quick action taken by the victim regarding reporting of committing the fraud increases the chance of recovery of the money duped by the cyber criminals.

Conclusion

The information and communication technology and cyberspace is dynamic in nature and the expansion of financial activities is also utmost crucial to fulfil the need of human beings. Thus, identifying, minimizing and taking preventive measures against such instances is not central and is decentralized among all i.e., the government, authorities and regulatory bodies (like:- RBI), citizens and the law enforcement mechanism. There is no doubt that the financial institutions have introduced somewhat rigid policies framework than before but has yet to work on the proper implementation of several other tactics and techniques in order to secure the cyberspace in regard of financial transactions. Financial institutions' main emphasis is to enhance control mechanism, manage the risk of fraud, and procure advanced processes for smooth and lesser fraud prone financial activities in cyber world. The RBI's Central Fraud Registry Portal, to which all the banks in India can have access, assists the banks to identify such fraud prone instances.

This isn't enough, as the upcoming era is completely going to be digitized the cybercriminals are more likely to attack the backbone of every nation's economy i.e., banking and financial sector. Thus, there is a need of raising awareness about cyber security among individuals and also proper allocation of budget for conduct of management and programs regarding cyber security in context of financial frauds in cyberspace. Also, there is a need of legislation dealing specifically with financial crimes in cyberspace as a separate class of offence.

References

(1) Isabel Arkvik, "What is financial cybercrime and how to prevent it?", October 27, 2021, https://www.visma.com/blog/what-is-financial-cybercrime-and-how-to-prevent-it/.

(2) Vijayalakshmi P, Priyadarshini V, Umamaheshwari K, "Impacts of Cybercrime on Internet Banking", International Journal of Engineering Technology and Management Sciences, Issue- 2 Volume-5, ISSN: 2581-4621, March 2021.

(3) Himanshi Lodha, Divya Mehta, "An Overview of Cybercrimes In Baking Sector", https://www.legalserviceindia.com/legal/article-7694-an-overview-of-cyber-crimes-in-banking-sector.html.

(4) Nihit Nagpal, Anuj Jhawar, "Remedies Available In Cases of Cyber Financial Frauds- India", 26th December 2022,

[110] Nihit Nagpal, Anuj Jhawar, "Remedies Available In Cases of Cyber Financial Frauds- India", 26th December 2022, https://www.mondaq.com/india/white-collar-crime-anti-corruption--fraud/1264828/remedies-available-in-cases-of-cyber-financial-frauds--india.

https://www.mondaq.com/india/white-collar-crime-anti-corruption--fraud/1264828/remedies-available-in-cases-of-cyber-financial-frauds--india.

(5) Zeshan Naz, "Cyber Security Threats in Banking: Importance, Threats, Challenges", 24th Jan. 2023, https://www.knowledgehut.com/blog/security/cyber-security-in-banking.

(6) Article on "What are the types of Cyber Attacks on Financial Institutions?", https://www.fortinet.com/solutions/industries/financial-services/types-of-cyberattacks-on-financial-institutions.