ABHIDHVAJ LAW JOURNAL

[www.abhidhvajlawjournal.com]

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Editor In chief – Assistant Professor Mr. Janmejay Singh

Publisher & Founder – Vaibhav Sangam Mishra

Frequency – Quarterly (4 Issue Per year)

ISSN: 2583-6323 (Online)

Guardians of the Digital Vault: A Comprehensive Examination of Financial Cybercrime Legislation and Enforcement Strategies.

AUTHOR'S NAME - Prerana Ghosh, BA.LL.B, Fourth Year.

INSTITUTION NAME - Chandigarh University.

CO-AUTHOR NAME - Palak Kapoor, BA.LL.B, Fourth Year.

INSTITUTION NAME - Chandigarh University.

ABSTRACT:

The evolution of technology has brought unprecedented opportunities and challenges, with financial cybercrime emerging as a critical issue globally. India has witnessed a paradigm shift in its legal landscape to combat cyber threats. The legislative framework governing cybercrimes, including financial cybercrimes, has evolved over the years. The Information Technology Act of 2000, and subsequent amendments serve as the cornerstone, defining offenses, penalties, and jurisdictional aspects related to financial cybercrimes. IT Act 2000 covers several offenses like impersonation and identity theft, material misrepresentation, publication for fraudulent purposes, vishing, cyberbullying, Phishing, credit card fraud or debit card fraud, etc. Enforcement mechanisms play a pivotal role in combating financial cybercrime. The collaboration between various agencies, such as the Cyber-crime Cells and the National Cyber-crime Reporting Portal, is examined considering their efforts to investigate and prosecute cybercriminals. However, there are some loopholes in the enforcement of financial cybercrime like there is a lack of regulation for fintech in India which led to several instances of fraud and data breaches in fintech companies. Despite commendable initiatives, challenges persist, ranging from the technical complexity of cyber investigations to the need for better international cooperation. Identifying challenges within the current system, the paper proposes recommendations for legislative improvements and emphasizes the need for a holistic approach to strengthen cybersecurity measures. Future trends and emerging threats are discussed to guide policymakers and law enforcement agencies in proactively addressing evolving challenges. In a comparative analysis, this paper juxtaposes India's legislative and enforcement framework with its international counterparts. By examining lessons learned from other jurisdictions, it offers recommendations for improving India's response to financial cybercrime. The importance of international collaboration in tackling cross-border cyber threats is emphasized, urging a collective effort to enhance global cybersecurity.

I. INTRODUCTION:

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it" as quoted by Stephane Nappo a Global Chief Information Security Officer at Group SEB.[1] Cyber incident can be defined as unauthorized access to a system's security policy which results in a cybercrime. With the increase in technological advancement, the risk of data leakage has been on the rise. As a result, credit card information and personal details related to bank accounts are stored in cold storage devices like Google Drive to avoid the loss of the financial health of an individual. Financial cybercrime is a criminal activity to obtain financial gain through fraudulent methods like stealing payment card information, identity fraud, email and internet fraud, etc. Financial cybercrime is not a new kind of threat, its history can be traced back not to just decades but even to centuries. The First cybercrime happened in 1834 in France even before the internet was intended. As there is an increase in digitization and automation of financial systems various techniques of cybercrime have evolved over a while. In the 1990s there was a rise in internet browsers due to which cybercriminals directly reveal the personal information of an individual or download viruses by a technique called domain spoofing[2]. The impact of financial cybercrime has been catastrophic, it results in the loss of trust and confidence of individuals which they have in their financial institutions. It also results in reputational damage to the banking sector as customers rely on banks to protect their financial and personal data. It has been observed that amount of network attacks has increased in recent years due to the impact of Artificial intelligence on society. Artificial intelligence can be defined as the computer's ability to act independently without human conduct. It paved the way for cybercriminals to clean up their language and provided new opportunities for hackers to break the computer network through emails by sharing personal information or by fabricating images or videos with the use of AI. The advancement in Artificial intelligence may also facilitate crimes like scamming, hacking, and money laundering. While discouraging the impact of AI it can be a helpful tool as it helps in detecting crime at its earliest stage by the use of AI technologies that recognize patterns and can even recognize minor behavior.

[1] blog.entrustit.co.uk, https://blog.entrustit.co.uk/why-cyber-security-and-company-reputation-go-hand-in-hand, (last visited Mar. 01, 2024).
[2] Andrew Douthwaite, Cybercrime's Evolution Since the 80's: Historical Facts and Figures, VIRTUAL ARMOUR (Feb 21,2024, 9:29 PM), https://virtualarmour.com/cybercrimes-evolution-since-the-80s/

I. HISTORICAL CONTEXT OF LEGISLATION GOVERNING FINANCIAL CYBERCRIME:

As far as computers have developed, so have also criminal offenses associated with their use.[3] The excessive use of computer networks in society develops new methods of inflicting crime due to which mankind will always have to live with criminal activity. Computer abuse is one of the criminal activities and as the name suggests any improper or illegal use of a computer to harm somebody can be termed as computer abuse. Intentionally infecting computers with a virus that will spread to other computers, using a computer to illegally share copyrighted items, cyberbullying, hacking, and identity theft are all examples of computer abuse. The legislation that governs these crimes are Computer Fraud and Abuse Act (CFAA) 1984 in which computer abuse was codified. The CFAA 1984 was amended to give comprehensive control over these cybercrimes and resulted in the enactment of The Computer Fraud and Abuse Act (CFAA) 1986 which imposes criminal penalties on the individuals who access the computers without proper authorization. It was operated by the US and some financial institutions and changes have been made continuously to expand its scope. It was further amended in 1994 in which civil penalty is incorporated along with criminal penalties.

II. EVOLUTION OF INFORMATION TECHNOLOGY ACT 2000:

In 1998 for the very first time, The Information Technology Bill was drafted by the Department of Electronics but it was introduced in the House in 1999. After witnessing substantial changes it was finally approved by the Union Cabinet on May 13, 2000, and by both Houses on May 17, 2000, Further, it received the Presidential assent on June 9, 2000, and thus it led to the formation of IT Act 2000. The Information Technology Act 2000 has a wider scope as it replaces the paper-based method of communication with communication through electronic mode.[4] It provides legal recognition to electronic commerce and to the transactions carried out by electronic data. It is a comprehensive legislation that is based upon The Indian Penal Code 1860 and The Indian Evidence Act 1872.[5] The purpose of IT Act 2000 is to elaborate on offenses, and penalties that

[3] Stein Schjolberg, The History of Global Harmonization on Cybercrime Legislation- The Road to Geneva, CYBER-CRIME HISTORY (Feb 23, 2024, 5:00 PM), https://cybercrimelaw.net/documents/cybercrime_history.pdf

[4] dhsgsu.edu.in, https://dhsgsu.edu.in/images/Reading-Material/Law/UNIT-IV-Second.pdf, (last visited Mar. 01, 2024).

[5] COMPUTER EDUCATION II UNIT IV, https://dhsgsu.edu.in/images/Reading-Material/Law/UNIT-IV-Second.pdf (Last visited Feb 24, 2024).

are related to cyber-crime, it also outlines the justice dispensation system for cyber-crimes. The Information Technology Act 2000 shall apply to all the documents and transactions specified in the first schedule except the documents or transactions like Negotiable Instrument as defined in The Negotiable Instrument Act, 1881 Trust as defined under The Indian Trust Act, 1882 or Power of Attorney as defined in The Power of Attorney Act 1882. The act defines certain offenses with their penalties like section 65 of IT Act 2000 deals with Tampering with computer source documents with a punishment of Imprisonment up to 3 years and or a fine of up to Rs200,000 likewise section 66 deals with Hacking with a computer system with a punishment of imprisonment up to 3 years or and with a fine up to Rs500,000 and many more. Due to the expansion of Information Technology services such as e-commerce, and e-transactions, the protection of personal data and information has been assumed to be of greater importance which requires coordination with the provision of the IT Act. To coordinate with the provisions of the Act, certain amendments are made to The Information Technology Act 2000 which are enshrined under Schedule 1 to 4. The first schedule has widened the scope of the term 'document' and includes within its meaning the ambit of electronic documents. The second schedule recognizes electronic documents as an admissible form of evidence under the Indian Evidence Act. One of the major amendments was made in 2008 in which Section 66A was introduced which penalized the sending of 'offensive messages' as there was a rapid increase in the use of computers which has given rise to new forms of crime such as video voyeurism, sexually explicit materials in electronic form, etc.[6]

III. TYPES OF FINANCIAL CYBER-CRIME:

Numerous types of cybercrime cause reputational or financial loss to an individual or to an organization. Financial cybercrime can range from fraud committed by a single individual to large-scale schemes organized by mastermind criminals. Some of the financial cyber-crimes are-

- Identity Theft – The act of obtaining personal information such as passwords, credit card numbers, or any sort of personal details related to finance and misusing them in

[6] *Id*, at. 1295.

the name of the victim for their economic gain can be termed as Identity theft. Since 1998, when Congress passed the Identity Theft and Assumption Deterrence Act,[7] Identity theft has been considered a federal crime.[8]

- Vishing- It is a crime that is conducted through voice communication in which attackers use phones to steal the personal information of the victim.[9] The most common example of Vishing is where attackers pretend to be a banker and convince the victim to transfer some money to their bank account, as soon as the victim logs in and transfers the money, all the access will be hacked by the attacker.
- Cyberbullying- It can be defined as using technology to harass, bully, or embarrass someone. It usually takes place through social media on devices like mobile phones, tablets, and computers.[10] It is somehow similar to Cyber defamation in which any act or gesture is designed to harm the person's reputation.[11] Examples- Posting embarrassing photos of someone on social media platforms or sending abusive messages through mobile phones.[12]
- Phishing- It is an attack perpetrated through e-mails.[13] It is an automated attack that happens when a victim clicks on any malicious link. The other names of Phishing are carding and brand spoofing in which the e-mail messages appear to be received from authorized businesses and are generally done by asking for the verification of certain information such as passwords and other personal details of a victim.[14] These messages look so official that 70% of the recipients may respond to them and ultimately bogged under the web of cybercrime.
- Cyber terrorism- It is defined as a purposive and politically motivated attack against any data or information that ultimately results in violence.[15] The intent behind the act is to create chaos among the public and to cease critical national infrastructure such as energy, transportation, government departments, military systems, etc.

[7] Dr. Amita Verma, CYBER-CRIMES AND LAW 308 (Central Law publications 2009).
[8] Dmitry Gorin, WHAT IS IDENTITY THEFT UNDER FEDERAL LAW?, thefederalcriminalattorneys, (Mar. 01, 2024, 9:29 PM), https://www.thefederalcriminalattorneys.com/identity-theft-federal-law
[9] IMPERVA, https://www.imperva.com/learn/application-security/vishing-attack/ (Last visited Feb 26, 2024).
[10] UNICEF, https://www.unicef.org/end-violence/how-to-stop-cyberbullying (Last visited Feb 26, 2024).
[11] DR. AMITA, *supra* note 4, at 1296.
[12] unric.org, https://unric.org/en/cyberbullying-what-is-it-and-how-to-stop-it/, (last visited Feb. 01, 2024).
[13] GEEKSFORGEEKS, https://www.geeksforgeeks.org/difference-between-phishing-and-vishing/ (Last visited Feb 26, 2024).
[14] DR. AMITA, *supra* note 4, at 1296.
[15] TECH TARGET, https://www.techtarget.com/searchsecurity/definition/cyberterrorism (Last visited Feb 27, 2024).

IV. ENFORCEMENT MECHANISM IN INDIA:

Enforcement plays a crucial role in combating financial cybercrime. Cyber–crime cells are the ones that keep track of tackling cyber-crime. Cyber-crime cells are a smaller version of the criminal investigation department in respective cities but these only deal with the issues related to the internet. According to the IT Act 2000, cybercrime has a worldwide jurisdiction which means cyber complaints can be filed in any of the cyber-crime cells in India irrespective of the place where crime took place. After a complaint is filed, an investigation has to be conducted by the cell and started with the search and seizure of digital evidence.[16] The investigating officer can be any police officer not below the rank of inspector. At first, the investigating officer has to look for a place where the computer or network of computers is found.[17] Advice given by technical experts can be referred to wherever necessary.

Raigarh Case – In this case, the SBI branch of Raigarh received an e-mail allegedly from Microsoft Support teams with the subject as 'Double your internet surfing speed'. The mail appeared to be so authentic and professional that the bank officials became confident that they had received it from a reliable source but ultimately it was a scam that was operated through a software named Dialup Security. Whenever any of the officials tries to surf the internet connection through Dialup networking, it captures the username and password and sends a mail to the sender of this program who keeps the record file in a directory named Akshdoot.doc. The bank complained about the hacking of their systems. Investigations revealed that Akshdoot was a project that was run by the Aptech Centre. When the police raided the Aptech Centre, they got all the sent emails and recorded data of the bank. The police have registered a case under section 66 of the IT Act 2000 for the offense of committing the crime.

CBI V/s Arif Asim[18] – In this case, the accused Arif Asim has stolen the credit card credentials of an American national and by using the details purchased a Sony Color Television set and cordless headphones from the website run by Sony India Ltd. After one and a half month, the credit card agency informed the company that the transaction was fraudulent and was done by

[16] Antalina Guha, How does cybercrime cell work in India, FINOLOGY BLOG (Feb 28, 2024, 3:00 PM), https://blog.finology.in/recent-updates/how-cybercrime-cell-works

[17] Dhiren Sehgal, How Does Cyber-crime Cell Work In India?, blog.ipleaders, (Mar. 01, 2024, 9:29 PM), https://blog.ipleaders.in/cyber-crime-cell-work-india/

[18] CBI V/s Arif Asim (Sony Sambandh Case), AIR 2003

an unauthorized person.[19] Thereupon the company complained to the CBI and initiated an investigation under sections 418, 419, and 420 IPC. The court convicted him of cyber fraud (section 66 C) of the IT Act 2000 and cheating.

State of Tamil Nadu V/s Suhas Katti[20] –In this case, the accused wanted to marry the victim, Ms. Roselind but she refused the proposal. In revenge for the rejection, the accused started harassing her by posting obscene messages in various groups, circulating her phone number, and creating a fake account in her name in order to disgrace her. The court found the accused guilty of the offense of forgery for the purpose of harming reputation under section 469IPC, word, gesture, act intended to insult modesty of a woman under section 509IPC and under section 67 of IT Act 2000 which deals with the publication and submission in electronic form that is against the will of a person and is to cause defamation.

V. CHALLENGES IN COMBATING FINANCIAL CYBERCRIME:

In the ever-evolving landscape of technology, financial cybercrime has become a pervasive and complex threat, requiring robust mechanisms for enforcement. Despite commendable efforts by authorities, several challenges persist, impeding the effective combat against these illicit activities.

- **Technical Complexity of Cyber Investigations:** One significant challenge lies in the intricate nature of cyber investigations. The rapid advancement of technology has empowered cybercriminals with sophisticated tools and techniques, making it challenging for law enforcement to keep pace. Encryption, anonymization, and decentralized networks create hurdles in tracing the origin of cybercrimes, hindering the identification and prosecution of offenders. To overcome this challenge, there is a growing need for continuous training and upskilling of law enforcement personnel. Investing in cutting-edge forensic technologies and fostering collaborations with cybersecurity experts can enhance the capabilities of agencies in navigating the intricate web of digital evidence.[21]

[19] studocu.com, https://www.studocu.com/in/document/jagannath-international-management-school/basics-of-new-media/cyber-crime-case-studies-unit-2/38791414, (last visited Mar. 01, 2024).
[20] State of Tamil Nadu V/s Suhas Katti, C No. 4680 of 2004
[21] civiceye.com, https://www.civiceye.com/metadata-in-digital-evidence-corroboration/, (last visited Mar. 01, 2024).

- **Need for Better International Cooperation:** Financial cybercrimes often transcend national borders, necessitating seamless collaboration between countries to apprehend perpetrators. The absence of standardized international protocols and legal frameworks poses a significant hurdle in effectively combating cross-border cyber threats. Jurisdictional complexities and varying legal systems hinder the timely exchange of information and coordination in investigations. To address this challenge, there is a crucial need for the establishment of international agreements and cooperation frameworks. Mutual legal assistance treaties (MLATs) and streamlined communication channels can facilitate the swift sharing of information and evidence across borders. A harmonized approach to cybercrime legislation at the global level can foster a more effective response to transnational financial cybercrimes.
- **Impact on Globalized Economy:** The interconnected nature of the global economy amplifies the repercussions of financial cybercrimes. Attacks on financial institutions, businesses, or critical infrastructure can have cascading effects, leading to economic instability. The interconnectedness also means that vulnerabilities in one region can be exploited to compromise systems worldwide, creating a systemic risk that requires a coordinated international response. Addressing this challenge involves not only strengthening domestic cybersecurity measures but also fostering international collaboration to fortify the resilience of the global financial ecosystem. Regular information sharing, joint threat intelligence initiatives, and coordinated response plans are essential components in mitigating the broader economic impact of financial cybercrimes.

VI. IMPORTANCE OF INTERNATIONAL COLLABORATION FOR INDIA:

In today's interconnected world, international collaboration is crucial for India to effectively address various global challenges, including combating financial cybercrime, promoting sustainable development, and fostering economic growth. This section specifically highlights India's engagement with international organizations, law enforcement agencies, and industry

partners to share best practices, exchange information, and strengthen the global fight against cyber threats.[22]

A. Cross-Border Nature of Cyber Threats:

- **Transnational Scope:** Financial Cybercrime transcends national borders, creating a complex environment for investigation and prosecution. Cybercriminals can easily exploit jurisdictional ambiguities, launching attacks from one country, targeting victims in another, and storing stolen data. This geographical dispersion poses significant challenges for individual nations, making international collaboration essential for effectively tracking and apprehending cybercriminals.
- **Sharing of Information and Expertise:** Collaborative efforts enable nations to share crucial information concerning cyber threats, including attack methods, and intelligence on cybercriminal activities. This information sharing allows countries to learn from each other's experiences, develop countermeasures more effectively, and prevent widespread harm.
- **Joint Investigations and Law Enforcement Operations:** International collaboration facilitates joint investigations and coordinated law enforcement operations across borders. This collaboration allows nations to pool resources, leverage diverse expertise, and apprehend cybercriminals across international jurisdictions.

B. Urgent Need for Global Cybersecurity Efforts:

- **Collective Defence:** The intricate and ever-evolving nature of cyber threats necessitates a global approach to cyber defense. No single nation possesses the resources or expertise to combat sophisticated financial cyberattacks alone. By forming alliances and engaging in multilateral cooperation, nations can combine their strengths, share intelligence, and develop collective strategies to protect critical infrastructure and ensure the stability of the global digital ecosystem.
- **Standardization of Best Practices:** Collaborative efforts allow for the standardization of best practices in cybersecurity across different nations. This standardization includes

[22] V. Thenmozhi , A. Karunamurthy , V. Vigneshwar, Understanding the Dynamics of Cybercrime in India a Comprehensive Study and Recommendations, Volume 12, IJSR, 173, 2023, Understanding the Dynamics of Cybercrime in India a Comprehensive Study and Recommendations (ijsr.net)

establishing common legal frameworks, developing harmonized cybercrime legislation, and promoting consistent cybersecurity hygiene practices. This helps create a more unified and effective front against cyber threats on a global scale.

- **Addressing Emerging Threats:** The rapid development of new technologies constantly introduces emerging cyber threats. Through international collaboration, nations can leverage collective research and development efforts to stay ahead of these evolving threats, fostering innovation in threat detection, prevention, and response capabilities (World Economic Forum, 2023).

C. International Conventions and Organizations

- **The Budapest Convention on Cybercrime:**

The Budapest Convention on Cybercrime, which was introduced for signature in Budapest, Hungary, in November 2001, is widely regarded as the most significant international treaty concerning cybercrime and electronic evidence.[23] The Budapest Convention provides for:

(i) the criminalization of conduct ranging from illegal access, data, and systems interference to computer-related fraud and child pornography;[24] (ii) procedural law tools to investigate cybercrime and secure electronic evidence in relation to any crime; and (iii) efficient international cooperation.[25] Practical experience shows that the Budapest Convention is more than a legal document providing for the criminalization of cybercrime, procedural powers to secure electronic evidence, and a legal basis for international cooperation.[26]

The increasing complexity of financial cybercrime and the challenges of securing electronic evidence pose significant hurdles for governments worldwide, jeopardizing justice and undermining faith in the rule of law.[27] While international efforts, such as the Council of Europe's Cybercrime Convention Committee (which represents the parties to the Budapest

[23] wikipedia, https://en.wikipedia.org/wiki/Convention_on_Cybercrime, (last visited Feb. 01, 2024).
[24] rm.coe.int, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, (last visited Feb. 01, 2024).
[25] THE BUDAPEST CONVENTION ON CYBERCRIME: BENEFITS AND IMPACT IN PRACTICE, 16809ef6ac (coe.int) (last visited March 1, 2024)
[26] *Id.* at. 1301.
[27] LISA BHANSAL, Defining our path to the 'Rule of Law', (Feb. 01, 2024, 4:19 PM), https://blogs.worldbank.org/governance/defining-our-path-to-the-rule-of-law

Convention on Cybercrime), seek solutions for accessing evidence in the cloud, India's non-participation limits its ability to shape future international solutions and share experiences.

So far, foreign policy considerations may have prevented India's accession to the Budapest Convention. Given the surge in financial cybercrime and the vision of a Digital India, it may be time for the government of India to reconsider its position.[28]

- **International Organisations:**

The various international organizations work at their best capacity in their territory to combat financial cybercrimes and protect themselves from all cyber threats. Some of these international organizations are:

1. NCSA (National Cyber Security Authority) -
   It prevents cyber threats and attacks in order to protect Rwanda's critical infrastructure, develops cybersecurity policies and strategies to ensure cyber resilience, oversees the implementation of the law relating to the protection of personal data and privacy, collaborates with different partners, such as institutions in the public and private sectors, law enforcement and security agencies, academia, and civil society, to ensure secure cyberspace, works with law enforcement agencies and the public to fight cybercrime.[29]

2. ENISA (European Union Agency for Cybersecurity) -
   Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.[30]

[28] INDIA AND THE BUDAPEST CONVENTION: WHY NOT, India and the Budapest Convention: Why not? (orfonline.org) (last visited March 1, 2024)
[29] NATIONAL CYBER SECURITY AUTHORITY, National Cyber Security Authority | About NCSA (last visited March 2, 2024)
[30] EUROPEAN UNION AGENCY FOR CYBERSECURITY, About ENISA - The European Union Agency for Cybersecurity — ENISA (europa.eu) (last visited March 2, 2024)

3. ITU (International Telecommunication Union) –

   An agency of the United Nations that is responsible for issues related to information and communication technologies. The ITU also works to combat cybercrime, and it has developed a number of tools and resources to help countries protect themselves from cyber threats.[31] ITU offers training programs and resources to help member states enhance their cybersecurity skills and knowledge, which benefits Indian professionals and organizations.

4. ICC (International Chamber of Commerce) –

   The International Chamber of Commerce (ICC) is the largest business organization in the world. It advocates for businesses and promotes international trade and investment. It provides a platform for businesses to address global challenges and shape policy. ICC advocates for strong cybersecurity policies at the international level, pushing for frameworks that protect businesses from cybercrime.[32]

Each of these organizations contributes to the global effort to combat financial cybercrime by providing support, expertise, and resources to countries like India. Collaboration between these entities, along with national authorities and private sector stakeholders, is crucial in developing effective strategies and frameworks to address the evolving cyber threats in the financial sector. India's success in combating financial cybercrime will significantly depend on its effective collaboration with international organizations and partners.

VII. COSMOS COOPERATIVE BANK: A CASE STUDY OF FINANCIAL CYBER-CRIME:

The Cosmos Cooperative Bank cyber-attack, which occurred in August 2018, stands as a significant case study in the realm of financial cybercrime in India. This elaborate heist, involving international collaborators and sophisticated techniques, highlights the vulnerabilities of financial institutions and the need for robust security measures.

[31] V. THENMOZHI, *supra* note 14, at 1303.
[32] exportsmitra, https://exportsmitra.com/docs/international-chamber-of-commerce-icc-and-its-role/, (last visited Feb. 6, 2024).

The Incident:

On August 11, 2018, Cosmos Bank, a cooperative bank headquartered in Pune, Maharashtra, witnessed a large-scale cyber-attack. Hackers deployed malware that compromised the bank's systems, allowing them to gain access to customer data, including debit card information. This stolen data was then used to create cloned debit cards, which were subsequently employed to withdraw a staggering ₹94 crore from ATMs across 28 countries and various locations within India over a very short period.

This case study delves deeper into the technical aspects of the attack, highlighting the vulnerabilities exploited and the intricate methods used to steal millions.

Phase 1: Initial Breach and Information Gathering:

The attack most likely began with an initial phishing email or a malware-laden website. These tactics are often used to gain a foothold within the bank's network, potentially tricking an employee into clicking on a malicious link or downloading infected software. Once initial access was established, the attackers likely employed lateral movement techniques to gain access to critical systems within the bank's network, including those involved in processing ATM transactions.

Weapon of Choice: Malicious Code and Code Injection:

The attackers are believed to have used malware specifically designed to target the bank's internal systems. This malware may have exploited known vulnerabilities within the bank's software or operating systems, allowing the attackers to gain administrative privileges and complete control over specific functions. A particularly concerning aspect of the attack involved the use of code injection. Once malware is inserted into the system, it sets up an ATM/POS proxy switch which is in parallel with the bank's own central switch, and the connection between the core banking system (CBS) and the bank's central switch is then redirected because of which the required messages to authorize debit card withdrawals never get forwarded to the core banking system.[33] This technique involves injecting malicious code into legitimate applications or scripts, essentially manipulating them to perform unauthorized

[33] Subhajit Routh, The potential of technological innovation to reduce fraud and increase trust in the Indian banking system, DUBLIN BUSINESS SCHOOL, 39 (2019), The potential of technological innovation to reduce fraud and increase trust in the Indian banking system (dbs.ie)

actions. In the Cosmos Bank case, the attackers reportedly injected malicious code into the bank's ATM switch, a crucial system responsible for routing communication between ATMs and the core banking system (CBS).

Bypassing Security and Fabricating Funds:

The injected code likely contained functionalities that deceived the ATM switch. Instead of routing withdrawal requests to the bank's core system for authorization, the malicious code likely bypassed this step, fabricating approval, and authorization signals, essentially allowing fraudulent transactions to proceed unchecked. This explains the rapid succession of unauthorized withdrawals observed across various countries.

Phase 2: International Transfer Attempt:

Following the successful ATM withdrawals, the attackers turned their attention to a larger heist. They attempted to initiate an unauthorized international transfer of a significant amount (₹13.92 crore) to a Hong Kong-based entity using the SWIFT (Society for Worldwide Interbank Financial Telecommunication) network. This network, crucial for international financial transactions, requires proper authentication and authorization procedures. Fortunately, the bank's SWIFT controls were robust enough to detect the suspicious activity and block the transfer, preventing further financial losses.[34]

Investigation and Aftermath:

The cyber-attack triggered a swift response from the authorities. The Pune City Police launched a comprehensive investigation, leading to the arrest of 18 individuals suspected of involvement in the crime. As of 2023, 11 of the accused have been convicted, while the remaining face ongoing legal proceedings. The judicial magistrate (first class) sentenced nine of the accused to four years imprisonment and two others to three years and imposed a fine on them.[35]

Key Learnings from the Case:

[34] indianexpress, https://indianexpress.com/article/cities/pune/cosmos-bank-malware-attack-pune-court-convicts-11-accused-8570830/, (last visited Feb. 6, 2024).
[35] THE HINDU, Pune court convicts 11 accused in Cosmos Bank cyber fraud case - The Hindu (last visited March 3, 2024)

The Cosmos Bank cyber-attack serves as a stark reminder of the evolving nature of cyber threats faced by financial institutions. According to the manager of Cosmos Bank, technological advancement is mainly responsible for newer ways to commit cyber fraud, and also, he mentioned that maybe countries like North Korea are becoming the main source from where these online frauds are getting organized.[36] This incident underscores the critical importance of:

- Implementing robust cybersecurity measures: Banks need to invest in sophisticated security systems, including firewalls, intrusion detection systems, and data encryption, to safeguard sensitive information. The Cosmos Bank has collaborated with tech giant Infosys to beef up the IT infrastructure and it has also enhanced the security measure for the ATM switch server and SWIFT server.[37]
- Regularly monitoring systems for suspicious activity: Continuous monitoring and vigilance are crucial for timely detection and mitigation of potential cyber-attacks.
- Raising customer and employee awareness: Educating customers and employees about cyber security best practices, such as using strong passwords and being cautious about suspicious emails or phone calls, can significantly reduce the risk of falling victim to social engineering tactics. After the Cosmos cyber-attack, the bank conducted training programs to spread awareness regarding cyber security among the employees.[38]
- Cooperation between law enforcement and financial institutions: Collaborative efforts between these entities are essential for effectively investigating and prosecuting cyber criminals

VIII. RECOMMENDATIONS FOR LEGISLATIVE ENFORCEMENT AND STRATEGIES:

Financial cybercrime poses a significant threat to India's growing digital economy. To effectively address this challenge, legislative improvements are crucial. Here are three key areas for recommended legislative action:

[36] SUBHAJIT, *Supra* note 21, at 1306.
[37] *Id*. at 1306.
[38] *Id*. at 1306.

A. Strengthening Fintech Regulations:

- **Regulatory Framework for New Technologies:** Establish a comprehensive regulatory framework for emerging financial technologies (fintech) like blockchain, artificial intelligence (AI), and cryptocurrency. This framework should balance innovation with consumer protection and mitigate potential risks associated with these technologies.
- **Cybersecurity Standards for Fintech Companies:** Mandate strong cybersecurity standards for all fintech companies operating in India. These standards should include requirements for data security, incident response protocols, and vulnerability management practices.
- **Know Your Customer (KYC) and Anti-Money Laundering (AML) Compliance:** Ensuring stricter compliance with KYC and AML regulations in the fintech sector is crucial. This includes enhanced customer verification processes, transaction monitoring, and reporting suspicious activities to relevant authorities.

B. Addressing Enforcement Challenges:

- **Specialized Cybercrime Courts:** If the speed of the criminal justice system is not commensurate with the rapid pace of developments in cybersecurity, it will embolden cybercriminals.[39] Thus, there is a need to establish specialized cybercrime courts with trained judges and staff who possess a deep understanding of cybercrime investigation and prosecution. This can streamline the judicial process and expedite cybercrime cases.
- **Enhanced Investigative Powers:** Equip law enforcement agencies with the necessary legal tools to effectively investigate cybercrime. This includes granting them the authority to access digital evidence, conduct cyber-forensics investigations, and collaborate seamlessly with international agencies in cross-border cases.
- **Harmonization of Cybercrime Laws:** Harmonize domestic cybercrime legislation with international legal frameworks like the Budapest Convention on Cybercrime. This

[39] THE HINDU, https://www.thehindu.com/business/india-may-require-special-courts-to-try-cybercrime-cases/article25083785.ece (last visited March 3, 2024)

ensures consistency in the definition, investigation, and prosecution of cybercrimes across jurisdictions.

C. Cybersecurity Awareness and Education: Invest in national awareness campaigns and educational programs to educate citizens about cyber hygiene practices, identify, and report suspicious activity, and make informed decisions in the digital environment. Public awareness initiatives shall be taken by the government, non-profit organizations, and private sector entities to educate individuals and businesses about online safety, responsible internet usage, and preventive measures to mitigate cyber risks.[40] By implementing some comprehensive strategies, India can equip its citizens with the knowledge and skills necessary to navigate the digital world confidently and become active participants in protecting themselves and the nation from financial cybercrime. Creating a well-informed and vigilant population is vital for building a resilient and secure digital ecosystem.

CONCLUSION:

India's digital landscape is flourishing, but a dark cloud threatens its growth: financial cybercrime. This pervasive threat employs sophisticated tactics, targeting both individuals and businesses, posing a significant risk to the nation's economic well-being. The consequences of financial cybercrime are far-reaching. It erodes public trust in digital transactions, discouraging individuals from participating in the digital economy, and impacting financial inclusion efforts. Furthermore, it deters foreign investment, hindering economic growth and jeopardizing India's position in the global digital ecosystem. Combating this multifaceted challenge requires a multi-pronged approach. Firstly, investing in cybersecurity infrastructure is crucial. This encompasses building well-protected cyber forensic capabilities and deploying cutting-edge technologies for threat detection and prevention. Additionally, building a skilled workforce is paramount. Upskilling and reskilling the workforce to address evolving cyber threats is vital for establishing a strong defense. Strengthening legal frameworks plays a critical role. Reviewing and updating existing legislation to address emerging threats and consider adherence to international conventions like the Budapest Convention can provide clarity and

[40] V. THENMOZHI, *supra* note 14, at 1308.

consistency in cybercrime prosecution. A**ctive international collaboration** is indispensable. Sharing information, participating in joint investigations, and adopting common cybercrime prevention strategies through collaboration with foreign counterparts are vital in tackling transnational criminal networks. The future of India's digital landscape is not one of fear but of empowerment. By embracing innovation and collaboration, India can transform the looming shadow of financial cybercrime into a catalyst for a secure and prosperous digital future. By prioritizing cybersecurity investments, nurturing skilled professionals, strengthening legal frameworks, and prioritizing public awareness, India can build a more resilient digital ecosystem, safeguard its financial sector, and pave the way for a safer and more secure future for its citizens and the overall economy.