CYBER FINANCIAL CRIME IN THE DIGITAL ERA: LEGAL CHALLENGES AND REGULATORY RESPONSES IN INDIA

Asst. Prof. Goutham Krishna K, Dr. Ambedkar Global Law Institute, Tirupati

ABSTRACT

Digital technologies have boomed which also means more people are using online financial systems. There are data up to October 2024: Digital payment platforms, online banking services, and electronic commerce have greatly improved financial accessibility and operational efficiency. Nevertheless, this shift to the digital world has also brought about new points of weakness that cybercriminals are targeting in order to commit monetary crimes. Identity theft, phishing, online banking fraud and ransomware attacks are examples of Cyber financial crime that pose a serious threat to individuals, companies and governments. The increasing prevalence of cybercrimes in India can be attributed to the exponential increase in digital financial technology adoption among its citizens. To examine the nature & evolution in cyber financial crime, assess its increasingly prevalent impact on digital economy of India and evaluate the efficacy of legal framework around Cybercrime in India. It specifically highlights the Information Technology Act, 2000 and other statutory provisions dealing with various forms of cyber finance crimes. It also highlights the weaknesses in the existing legal system and suggests that more robust legislative measures, better cybersecurity infrastructure, and increased public awareness are needed to adequately address cyber financial crimes.

Keywords: Cybercrime, Financial Cybercrime, Digital Fraud, Identity Theft, Phishing Attacks, Online Banking Fraud, Cybersecurity Law, Information Technology Act 2000, Cybercrime in India, Digital Financial Security, Cyber Fraud Prevention.

INTRODUCTION

Digitalizing financial services is the most successful and transformative face of modern economic systems that can speed up transaction process, expand the frontiers of financial inclusion and increasing access to financial resources. Aspects such as online banking, mobile payment solutions and thousands of ecommerce web establishments have become part of modern-day monetary systems. While these benefits exist, the growth of digital financial infrastructure has also been met by cybercriminals activities. As a result, cybercrime has become one of the greatest threats to the stability and security of digital economies.[1]

Cybercrime encompasses a broad range of criminal enterprises involving the use of computer technology, networks, or digital systems to either aid in committing offenses, or as beneficial targets for criminal action. According to the United States Department of Justice, a cybercrime is a crime that requires knowledge and utilization of computer technology for its perpetration, investigation, or prosecution.[2] Likewise, international institutions highlight that cybercrime is transnational because, through digital networks, perpetrators can commit crimes remotely or in a jurisdiction different from where the crime takes place.[3]

The Information Technology Act, 2000 was India's first comprehensive legislation addressing cybercrime and electronic transactions. The Act offers legal validity of electronic records, digital signatures, and E-commerce while also laying down penal provisions against cyber crimes.[4] It also amended the traditional laws like the Indian Penal Code now BNS, the Code of Criminal Procedure now BNSS and the Indian Evidence Act now BSA to make provisions for digital crimes and electronic evidence.[5] However, the continued evolution of cybercriminal activities presents significant challenges to the adequacy and effectiveness of existing legal frameworks.

Financial cybercrime is especially worrying because it directly attacks financial assets and economic systems. Cybercrime: Cybercriminals seek vulnerabilities in technology to access financial data, steal it or otherwise facilitate illegal transactions. How Identity Theft, Phishing

[1] P.A. Watters, Cybercrime and Cybersecurity 200 (1st ed. 2024).
[2] U.S. Department of Justice, Definition of Cybercrime (describing cybercrime as violations of criminal law involving computer technology)
[3] P.T. Ortese, An Analysis of the Nature and Scope of Cybercrime, 1 Cavendish Univ. L.J. 179–193 (2022).
[4] Information Technology Act, No. 21 of 2000, § 1 (India).
[5] Indian Penal Code, No. 45 of 1860 (India); Code of Criminal Procedure, No. 2 of 1974 (India); Indian Evidence Act, No. 1 of 1872 (India).

Attacks, Credit Card Fraud, Online Banking Fraud, Ransomware Attacks and Cyber Extortion Are All Related to Cyber Crime[6] With the rise in digital financial transactions in India, cyber financial crimes have emerged as a major concern for policymakers, law enforcement agencies and financial institutions**.**

EVOLUTION OF CYBER FINANCIAL CRIME

The evolution of cyber financial crime echoes behind the generative phenomenon related to technological advancement along with increasing embedment of digital systems into financial engines. At the dawn of the internet age, cybercrime involved illegal entry into computer systems and primitive hacking. However, over the years, cybercriminal behavior has become much more organized and technologically advanced involving sophisticated malware and social engineering tactics as well as multinational crime syndicates.[7]

Ransomware Attacks Have Increased Massively one of the Biggest Development In Cybercrime Ransomware attacks use malicious software to encrypt the victim's data and demand payment in order to restore access to the system. Such attacks can have a devastating impact on business processes and our essential public infrastructure, resulting in millions of euros damage to bodies corporate and reputational harm.[8]

Identity theft is another major cyber financial crime on the rise. Cyber criminals steal sensitive data such as bank login details, addresses or social security numbers in identity theft cases and use that info to perform bogus transactions or open fraudulent financial accounts. Only a major loss of funds alerts victims to the fact that they have been robbed.[9]

Phishing is yet another common method used by cybercriminals as well. Phishing attacks are where fake messages or emails that pretend to be from a legitimate institution such as a bank or a financial service provider. Victims are lured into disclosing sensitive information such as passwords, credit card numbers or one-time passwords.[10]

As mobile device usage has risen, it has opened up even more opportunities for cybercriminals

---

[6] Visma, What Is Financial Cybercrime and How Can We Prevent It? (2025), https://www.visma.com/resources/content/what-is-financial-cybercrime-and-how-to-prevent-it.html.
[7] Cybersecurity Ventures, The History of Cybercrime and Cybersecurity: 1940–2020 (2020).
[8] International Monetary Fund, Global Financial Stability Report (IMF 2025).
[9] Kaspersky, What Is Cybercrime and How to Protect Yourself (2025), https://www.kaspersky.com/resource-center/threats/what-is-cybercrime-and-how-to-protect-yourself.
[10] Encyclopaedia Britannica, Cybercrime, https://www.britannica.com/topic/cybercrime.

in recent years. The smartphones and digital payment applications that store vast amounts of personal and financial data are a natural target for cybercriminals. Mobile phishing attacks are one of the most common forms of cyber fraud incidents, according to studies conducted around 2023.[11]

CYBER FINANCIAL CRIME STATISTICS IN INDIA

Cybercrime statistics show alarming figures for the rise of cyber financial crimes in India. Cybercrimes have seen a significant increase due to the exponential growth of digital financial services and penetration of internet, National Crime Records Bureau (NCRB) says. As per data, a total of 65,893 cybercrime cases in India were registered as compared to 52,974 cases reported in the year 2021. This is an increase of about 24.4 percent.[12]

Financial fraud is the most common case of cybercrime. According to data from the National Crime Records Bureau (NCRB), around 64.8 percent of cybercrime incidents are said to fall under the category of financial fraud, followed by extortion and other cyber-related crimes. Financial Fraud[13] The dominance of Financial fraud shows that as far as motives are concerned Most of the cybercriminal activities were financially motivated.

Table 1

Registered Cybercrime Cases in India

Year	Number of Registered Cases	Percentage Increase
2021	52,974	—
2022	65,893	24.4%
2023	86,420	31.2%
2024	1,01,928	17.9%

The economic impact of cybercrime is equally significant. Reports indicate that cybercriminals defrauded individuals and organizations of approximately ₹33,165 crore between 2021 and 2024.[14] In 2024 alone, cybercrime-related financial losses amounted to approximately ₹22,812

[11] Ministry of Finance, Government of India, Cyber Security and Fintech Report (2025).
[12] National Crime Records Bureau, Crime in India Report 2022 (Gov't of India).
[13] Press Information Bureau, Government of India, Cyber Fraud Cases Registered Under NCRB (2024), https://pib.gov.in.
[14] Indian Express, Rise in Cybercrime Cases: NCRB Report Highlights Financial Fraud (2025).

crore.[15]And in 2025 the amount was Rs.22,495 crore[16]

Table 2

Estimated Financial Loss Due to Cybercrime in India

Period	Estimated Financial Loss
2021–2023	₹10,353 crore
2024	₹22,812 crore
2025	22,495 crore
Total (2021–2025)	₹55,660 crore

One of the most significant trends in cybercrime is the rapid rise in complaints lodged via online cyber-crime reporting platforms. According to approximately 137,254 complaints were registered through the National Cyber Crime Reporting Portal in 2021. This had increased significantly to over 1.7 million complaints by 2024.[17] By 2025 it has reached up to 2.4 million.[18] Such a dramatic increase demonstrates not only an increase in cybercrime activity, but also citizens' awareness about reporting potential deficiencies (the statics available show more on the latter point).

TYPES OF CYBER FINANCIAL CRIMES

Cyber financial crimes encompass a wide range of illegal activities targeting digital financial systems. These crimes exploit technological vulnerabilities to gain unauthorized access to financial resources or personal data.

Table 3

Major Types of Cyber Financial Crimes

[15] Frost & Sullivan, Union Budget 2025 Prioritizes Cybersecurity Amid Rising Threats (2025).
[16] See Bandi Sanjay Kumar, Minister of State for Home Affairs, Rajya Sabha Question Response on Cyber Fraud Complaints and Losses (Feb. 2026), reported in The Indian Express and India Today (stating that Indians lost Rs 22,495 crore to cyber fraud in 2025).
[17] Business Standard, Indian Entities May Lose ₹20,000 Crore to Cybercrimes in 2025: CloudSEK (2025).
[18] Ministry of Home Affairs, Govt. of India, National Cyber Crime Reporting Portal (reporting approximately 24,02,579 complaints in 2025).

Type of Crime	Description
Hacking and Unauthorized Access	Illegal access to computer systems to steal or manipulate financial data
Identity Theft	Misuse of personal information to commit financial fraud
Phishing	Deceptive communication used to obtain sensitive financial information
Credit/Debit Card Fraud	Unauthorized use of card details to conduct transactions
Online Banking Fraud	Fraudulent access to bank accounts or digital payment platforms
Cyber Extortion	Threatening individuals or organizations for financial gain

Hacking and unauthorized access is one of the oldest types of cyber financial crime. Under Information Technology Act activities accessing computer systems such as unauthorized access and damage or loss to the property of a person that without all computing devices are included.[19]

Another key cyber financial crime is identity theft. This crime includes fraudulently using another individual's electronic signature, password, or identifier credentials to perform financial transactions. The poaching of user credentials can be punishable under Section 66C of the Information Technology Act, which criminalises identity theft and lays down punishment in terms of a jail term and monetary fines:[20]

Phishing attacks and their variants are also common, which commonly entails deceiving victims into disclosing sensitive information like bank or account login credentials. Cybercriminals frequently use fictitious websites or fake emails to trick victims into providing sensitive financial information.[21]

As digital payment platforms have proliferated, online banking fraud has also become more common. Fraudsters break into banking systems using malware attacks, phishing schemes, or

[19] Information Technology Act, 2000, § 43 (India).
[20] Information Technology Act, 2000, § 66C (Identity Theft) (India).
[21] Information Technology Act, 2000, § 66D (Cheating by Personation Using Computer Resources) (India).

identity theft allows them to move money or alter financial transactions.[22]

LEGAL FRAMEWORK GOVERNING CYBER FINANCIAL CRIME IN INDIA

India's primary legislation addressing cybercrime is the Information Technology Act, 2000. The Act provides legal recognition for electronic transactions and establishes penalties for cyber offenses involving unauthorized access, data theft, and online fraud.[23]

Table 4

Key Legal Provisions Addressing Cybercrime in India

Legal Provision	Description	Punishment
Section 43	Unauthorized access to computer systems	Compensation for damages
Section 65	Tampering with computer source documents	Up to 3 years imprisonment
Section 66	Computer-related offenses including hacking	Up to 3 years imprisonment
Section 66C	Identity theft	Up to 3 years imprisonment
Section 66D	Cheating by impersonation using computer resources	Up to 3 years imprisonment

Although the Information Technology Act provides the primary legal framework for addressing cybercrime, it operates alongside other laws such as the Bharatiya Nyaya Sanhita (BNS), which includes provisions related to cheating, forgery, and fraud. These laws collectively form the legal basis for prosecuting cyber financial crimes in India.[24]

[22] Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, Government of India.
[23] Information Technology Act, No. 21 of 2000, INDIA CODE (2000), https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.
[24] Indian Penal Code, No. 45 of 1860, §§ 415, 420, 463, 468, 471 (India); Information Technology Act, No. 21 of 2000, INDIA CODE (2000),

CHALLENGES IN COMBATING CYBER FINANCIAL CRIME

While legal frameworks are in place, the effective prevention and prosecution of cyber financial crimes facing significant barriers in India. One of the biggest problems is that cybercrime incidents are underreported. Cybercrime never reports many victims because of lack of knowledge, fear of goodwill damage, uncertainty on the legal process.[25]

A major obstacle is the absence of technical know-how in law enforcement agencies. Cybercrime investigations also demand specialized skills in areas such as digital forensics, data analysis, and cybersecurity that may not always be present within traditional law enforcement organizations.

Jurisdictional issues further complicate these investigations of cybercrime where the criminal is almost always operating from different countries. Indeed, this transnational nature of cybercrime creates significant hurdles to identifying offenders and bringing them to justice across national boundaries.

CONCLUSION AND FUTURE IMPLEMENTATIONS

Advancements in digital technologies have had huge impacts on the global financial system, making it possible for quicker transactions, greater financial inclusion and better access to financial services portfolio. But these advancements have also opened up new avenues for cybercriminal activity, especially on financial cybercrime. With the rise of digital platforms for banking, commerce, and communication the need for better anti-fraud has increased and as such cybercriminals are employing more technologically savvy methods to commit fraud ranging from phishing through identity theft, online banking fraud to cyber extortion. The emergence of these crimes has grave implications not only for people and businesses but also for the stability and integrity of digital financial systems.

The increasing penetration and acceptance of digital payment systems, mobile banking applications, and online financial services in the Indian scenario has amplified exposure to cyber financial crimes. The number of incidents of cybercriminal activity has been growing by leaps and bounds over the last few years, with those involving financial fraud in particular

---

https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

[25] See, e.g., R. Venkatasubramanian, Cybercrime in India: Challenges of Underreporting and Enforcement, 7 J. Indian L. & Soc'y 45, 48–50 (2016).

showing increased activity according to statistical data. The need for enhancing cybersecurity mechanisms and empowering institutions to better prosecute cybercrimes is exemplified by the rising number of complaints related to cybercrime as well as victims losing money.

In India, the Information Technology Act, 2000 is the main legislation for combating cybercrime. Although the Act legally recognizes electronic transactions and prescribes punishment for various cybercrimes, its provisions often lag behind fast-paced technological advancements and cunning tactics of cybercriminals. Moreover, other concerns like underreporting of cybercrime cases, limited technical expertise of law enforcement agencies, and jurisdictional challenges impede effective implementation of cyber laws.

Hallmarks of industry best practices The fintech industry is not yet mature, so what constitutes "best practice" for risk management within the cyber financial crime domain should be derived from and implemented in the world-leading sectors that have much higher precedents set for establishing best practices. Developing legislative structures, enhancing cybersecurity infrastructures, increasing digital literacy awareness, and fostering collaboration on international efforts are necessary to mutually ensure a safe and reliable cyberspace. This sort of integrative approach is key to addressing the risks associated with cyber financial crimes and maintaining digitally sustainable financial systems long term.