Proceedings of International Conference on "Recent Innovations in Engineering, Technology & Science for Sustainable Development (RIETSSD-2026)"
Career Point International Journal of Research (CPIJR)
 | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

Understanding Cybercrime Evolving Legal and Regulatory Framework for Combating Financial Fraud in India

Chandra Deep Singh[1], Dr. Mithlesh Malviya[2]

[1]Research Scholar, School of Legal studies and Governance, Career Point University, Kota (Rajasthan)

[2]Research Supervisor, School of Legal studies and Governance, Career Point University, Kota(Rajasthan)

Abstract

In the fast-changing digital era, cyber-enabled money laundering has become a pressing threat to national security and financial integrity. Since the development of the internet and technology, cybercrimes keep increasing. With new technological developments happening, everyday there is something new to add to the crime list. New laws were required to deal with this widespread problem. The purpose of this article is to examine cybercrime in India and the legal frameworks governing it to keep such crimes under control. With the rapid development of computer technology and internet over the years, the problem of cyber crime has assumed gigantic proportions and emerged as a global issue. It has created an entirely new set of problems for law enforcement agencies all over the world. It has equally become cause of serious concern for the legal fraternity to find effective ways and means to combat cyber criminality because of its worldwide devastating effect. Cyber security provides protection to the internet connected networks and system from the cyber-attacks. To stop attacks everyone must know and aware of all cyber law, regulations and compliance to secure the cyber. Cyber security is all about to stop cyber-crime. Cyber security is must and we have to know about all safety measures required to stop cyber-crime. Securing online information is priority where everyone is involved with technology. Whenever anyone talked about cyber security, straight one thing comes in mind that is cyber-crime and what safety measures need to take to be safe from it. Various legal regimes have tried their best to bring provisions to combat the issue.

Key words: Cybercrimes, global perspective, digital future, financial fraud, legal frameworks

Introduction

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

Financial fraud represents a persistent threat to economic stability, undermining trust among businesses, investors, and the general public. As India's financial ecosystem expands and transactions become increasingly sophisticated, the need for a robust regulatory framework to combat fraudulent activities has become paramount.

This discussion delves not only into India's evolving legal and regulatory landscape for addressing financial fraud but also offers insight into its historical development, key legislative milestones, and implications for forensic auditors operating in a digitally transformed financial environment.

India's formal financial institutions originated in the 19th century with the establishment of the Presidency Banks, which were later unified as the Imperial Bank of India in 1921. The establishment of the Reserve Bank of India (RBI) in 1935 centralized monetary control and oversight. Following independence, the Banking Regulation Act of 1949 expanded the RBI's authority, while the Securities and Exchange Board of India (SEBI), established in 1988, strengthened capital market governance. To meet sector-specific needs, the Insurance Regulatory and Development Authority of India (IRDAI) and the Pension Fund Regulatory and Development Authority of India (PFRDA) were established in 1999 and 2003, respectively. These developments mirrored the rapid growth and complexity of India's financial sector.

Recent legislative advancements have reinforced anti-fraud mechanisms. The Companies Act, 2013 introduced stringent provisions to curb corporate fraud. In 2023, the enactment of the Bharatiya Nyaya Sanhita and Bharatiya Sakshya Adhiniyam modernized India's criminal and evidentiary laws, replacing the Indian Penal Code (1860) and the Indian Evidence Act (1872), respectively, to better address contemporary financial crimes. Complementing these legal reforms, the Institute of Chartered Accountants of India (ICAI) issued the Forensic Accounting and Investigation Standards (FAIS) in 2023, providing a structured methodology and ethical framework for forensic professionals.

Understanding this regulatory evolution is crucial for professionals responsible for preventing, detecting, and investigating financial fraud in an era where digital banking and artificial intelligence are transforming the landscape of financial crime. India's legal

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

framework for combating financial fraud is multifaceted, involving various laws and regulatory bodies.

Development of cybercrimes in global context

On the advent of a large number of cyber crimes, many nations have felt the need to have some control mechanism. In order to combat the challenges posed by cybercrime, many countries have beefed themselves up against such crime. A number of countries have introduced extensive amendments to their substantive criminal law. These are USA, Austria, Denmark, France, Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada and Japan. The United States especially has made numerous amendments to their existing legislation. India, Spain, Portugal, UK, Malaysia and Singapore have made new enactment to prevent computer-related crime. Apart from fine, the punitive deterrents range from imprisonment from one year to ten years depending upon the gravity of the offence. Unauthorized access to computer/data/program has been classified as computer crime/offence by almost all the countries that have either enacted new statutes or amended existing criminal laws. Many countries have commenced to enact laws related to Digital Signature. The Convention on Cybercrime at Budapest was the first-ever international treaty on criminal offences committed against or with the help of computer networks such as the internet. The Convention deals in particular with offences related to infringements of copyright, computer-related fraud, child pornography and offences connected with network security. It also covers a series of procedural powers such as searches of an interception of material on computer networks. Its main aim, as set out in the Preamble, is to pursue "a common criminal policy aimed at the protection of society against cybercrime, inter-alia by adopting appropriate legislation and fostering international cooperation[1]."

It has an Additional Protocol making it a criminal offence to disseminate racist or xenophobic propaganda via computer networks. The treaty has a threefold aim: to lay down common definitions of certain criminal offences relating to the use of the new technologies, to define methods for criminal investigations and prosecution, and to define methods for international communication. The criminal offences concerned are: those committed against the

[1] Text of the council on Europe's convention on cybercrime treaty, budapest, available at, 2001. https://www.aclu.org/legal-document/text-councileuropes-convention-cybercrime-treaty l

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

confidentiality, integrity and availability of computer data or systems (such as the spreading of viruses); computer-related offences (such as virtual fraud and forgery); content-related offences (such as the possession and intentional distribution of child pornography); offences related to infringements of intellectual property and related rights. Another objective is to facilitate the conduct of criminal investigations in cyberspace, thanks to a number of procedural powers, such as the powers to preserve data, to search and seize, to collect traffic data and to intercept communications[2].

The European Union has set up an agency to coordinate work to combat the rising tide of cybercrime. The European Network and Information Security Agency will help educate the public about viruses, hacker attacks and other security problems. It will also act as a coordinator for Europe-wide investigations into virus outbreaks or electronic attacks[3].

Most Western countries have initiated some kind of anticybercrime capability or legislation, but this is slow to develop. In 1997 the UK established the Internet Crime Forum, bringing together police, government, prosecutors, internet industry officials and lawyers to discuss issues of mutual concern Canada looks likely to follow suit in light of the May 2000 G-8 meeting on cybercrime. Many other computer crime units are being established around the world. The FBI, for example, established its C-37 unit in 1996; the Russian Federal Security Service has established a system to monitor e-mail codenamed SORM (System of Operational and Investigative Measures). The G-8 currently has a high-tech crime group developing best practices for investigating online crime. The Council of Europe has drafted a convention on cybercrime, which aims to enhance powers to investigate and prosecute cybercrimes. More than 100 countries do not have the laws to deal with computer-related crime, including at least 60% of Interpol members. This has a huge impact on a country's own ability to combat cybercrime and on its ability' to assist other countries with their investigations. The hampering of the US-Philippine hunt for the perpetrator of the 'I Love You' virus was a prime example of this. There is a clear need to establish special communication channels that should always be open to process urgent and critical cases, as well as to enhance intelligence cooperation and coordination worldwide. The country's

[2] Henrik WKK aspersen. Cyber Racism and the Council of Europe's reply available at https://www.humanrights.gov.au/our-work/cyberracism-and-council-europes-reply
[3] EU hi-tech crime agency created, 12:55 GMT available at, 2003. http://news.bbc.co.uk/2/hi/technology/3226178.stm

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

authorities at the UN digital summit have defended Iran's policy of blocking access to certain websites. Iranian authorities claim only sites not compatible with Islam are blocked[4] .

Criminal Law Regime and Evidentiary Standards

Having gone into effect from July 2024, India has transitioned to a new criminal justice framework comprising:

- Bharatiya Sakshya Adhiniyam (BSA), 2023 – replacing the Indian Evidence Act, 1872.
- Bharatiya Nyaya Sanhita (BNS), 2023 – replacing the Indian Penal Code, 1860.

For forensic auditors, this shift has significant implications for how evidence is collected, preserved, presented, and evaluated in courts of law.

The BSA, 2023, introduces a technologically forward and litigation-friendly evidentiary regime. The BSA introduces several presumptions relevant to forensic practice:

- Presumption of authenticity for certified copies of public documents (Sections 78–83)
- Presumption of validity for electronic signatures and power of attorney (Sections 84–87)
- Presumption of genuineness for 30-year-old physical documents and five-year-old electronic records (Sections 92–93)
- Admissibility of Electronic Evidence:
    a) Electronic records such as emails, logs, spreadsheets, and metadata are admissible as primary evidence if properly authenticated.
    b) Forensic auditors must document every step of evidence handling—from acquisition to analysis—to ensure the integrity of the evidence.
    c) This presumes validity of certified electronic records older than five years, provided they are unaltered and properly stored.

[4] Aaron Scullion. Iran's president defends web control, 10:31 GMT available at, 2003. http://news.bbc.co.uk/2/hi/technology/3312841.stm

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

The BNS, 2023, consolidates and modernizes offenses previously scattered across the IPC. Key provisions relevant to forensic auditors showing in table 1:

Table 1: Key provisions relevant to forensic auditors

Section 316	Criminal breach of trust – misappropriation of entrusted property
Section 317	Breach of trust by public servant, banker, merchant, or agent – a critical provision in banking and corporate frauds
Section 318	Dishonest misappropriation of property – applicable in embezzlement cases
Section 320–323	Cheating and dishonestly inducing delivery of property – often linked to financial statement fraud
Section 336	Forgery and use of forged documents – relevant in document tampering and fake invoicing
Section 344	Falsification of accounts – central to forensic accounting investigations
Section 111	Organized crime—explicitly includes cyber extortion, phishing, identity theft, and botnet operations.

These provisions provide the legal basis for prosecution and must be referenced in forensic audit reports submitted to investigative agencies or courts.[5]

Acts amended by information technology act, 2000

The Indian penal code, 1860

Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended many time since, it covers almost all substantive aspects of criminal law and is supplemented by other criminal provisions. In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well. ITA 2000 has amended the sections dealing with records and

[5] https://www.jdsupra.com/legalnews/understanding-india-s-evolving-legal-3561980/

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

documents in the IPC by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as electronic record and electronic document thereby bringing within the ambit of IPC, all crimes to an electronic record and electronic documents just like physical acts of forgery or falsification of physical records. In practice, however, the investigating agencies file the cases quoting the relevant sections from IPC in addition to those corresponding in ITA like offences under IPC 463,464, 468 and 469 read with the ITA/ITAA Sections 43 and 66, to ensure the evidence or punishment stated at least in either of the legislations can be brought about easily.

The Indian evidence act 1872

This is another legislation amended by the ITA. Prior to the passing of ITA, all evidences in a court were in the physical form only. With the ITA giving recognition to all electronic records and documents, it was but natural that the evidentiary legislation in the nation be amended in tune with it. In the definitions part of the Act itself, the "all documents including electronic records" were substituted. Words like 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations. Admissibility of electronic records as evidence as enshrined in Section 65B of the Act assumes significance. This is an elaborate section and a landmark piece of legislation in the area of evidences produced from a computer or electronic device.

Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied:

- The computer output containing the information was produced by the computer during the period over which the computer was used regularly by lawful persons.
- The information derived was regularly fed into the computer in the ordinary course of the said activities;

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

- Throughout the material part of the said period, the computer was operating properly and a certificate signed by a person responsible, etc.

To put it in simple terms, evidences (information) taken from computers or electronic storage devices and produced as print-outs or in electronic media are valid if they are taken from system handled properly with no scope for manipulation of data and ensuring integrity of data produced directly with or without human intervention etc and accompanied by a certificate signed by a responsible person declaring as to the correctness of the records taken from a system a computer with all the precautions as laid down in the Section. However, this Section is often being misunderstood by one part of the industry to mean that computer print-outs can be taken as evidences and are valid as proper records, even if they are not signed. We find many computer generated letters emanating from big corporates with proper space below for signature under the words "Your faithfully" or "truly" and the signature space left blank, with a Post Script remark at the bottom "This is a computer generated letter and hence does not require signature". The Act does not anywhere say that 'computer print-outs need not be signed and can be taken as record'.

Banking Regulation Act, 1949 gives the RBI powers to inspect banks (Section 35), issue directions in the public interest (Section 36), penalize false statements fraud (Section 46), and remove top officials (Sections 10B / 10BB). RBI mandates forensic audits in cases of loan frauds exceeding ₹50 crore, non-performing asset manipulation, or wilful default and fund diversion. RBI's Master Directions on Fraud Risk Management, revised in July 2024, mandates early detection, reporting, and governance for banks, cooperative banks, and non-banking financial companies (NBFCs). These include Early Warning Systems (EWS) integrated with core banking solutions and Red Flagged Accounts (RFA) reporting.

Insurance Act, 1938: Under Section 33, the Insurance Regulatory and Development Authority of India (IRDAI) holds the authority to direct investigations into the affairs of insurers, reinsurers, and intermediaries to ensure compliance with regulatory norms and protect policyholder interests. These investigations encompass scrutiny of underwriting practices, claims settlement procedures, solvency margins, and grievance redress mechanisms. The IRDAI's Insurance Fraud Monitoring Framework, issued in 2013,

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

requires insurers to follow due diligence, establish risk management committees, and have board-approved fraud detection policies. It addresses both hard and soft frauds, such as exaggerated claims, to protect policyholders. In recent years, IRDAI has actively investigated cases of mis-selling, claim-denial irregularities, and data privacy breaches, reinforcing its role as a vigilant regulator in the insurance sector.

Companies Act, 2013

The Companies Act, 2013 is the principal legislation governing corporate conduct in India. It provides the statutory basis for fraud detection, auditor responsibilities, and investigative mechanisms.

- **Section 447** defines "fraud" in a broad manner. It encompasses any act, omission, concealment of a fact, or abuse of position committed with the intent to deceive, gain an undue advantage, or injure the interests of the company or its stakeholders. This provision applies even in the absence of actual wrongful gain or loss. This section is frequently cited in forensic audit reports submitted to regulators and courts, and it forms the legal basis for prosecution in corporate fraud cases.
- **Section 143** outlines the powers and responsibilities of statutory auditors, including mandatory inquiries into loans, advances, deposits, and the disposal of assets. It also imposes an obligation to report material fraud to the Central Government and immaterial fraud to the company's board of directors or audit committee and to opine on the adequacy of internal financial controls and compliance with accounting standards.
- **Section 138** mandates internal audits for certain classes of companies, including listed entities and large private companies. Internal auditors often serve as the first line of defense in detecting red flags that may later be escalated to forensic auditors.
- **Section 212** empowers the Central Government to assign cases of serious fraud to the Serious Fraud Investigating Officer (SFIO). Once a case is assigned, no other agency may investigate it, ensuring centralized and specialized handling of the case. SFIO reports are treated as police reports under the Bharatiya Nyaya Sanhita (BNS), 2023, and are admissible in court without the need for further investigation

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

by police authorities. Investigations can be initiated under this section based on reports from the Registrar of Companies or inspectors under Section 208, special resolutions passed by companies, requests from other government departments, or through Suo motu action by the Central Government.

The bankers' books evidence (BBE) act, 1891 Amendment to this Act has been included as the third schedule in ITA. Prior to the passing of ITA, any evidence from a bank to be produced in a court, necessitated production of the original ledger or other register for verification at some stage with the copy retained in the court records as exhibits. With the passing of the ITA the definitions part of the BBE Act stood amended as: "'bankers ' books' include ledgers, day-books, cash-books, accountbooks and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device". When the books consist of printouts of data stored in a floppy, disc, tape etc, a printout of such entry certified in accordance with the provisions to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons; the safeguards adopted to prevent and detect unauthorized change of data to retrieve data that is lost due to systemic failure or In short, just like in the Indian Evidence Act, the provisions in Bankers Books Evidence Act make the printout from a computer system or a floppy or disc or a tape as a valid document and evidence, provided, such print-out is accompanied by a certificate stating that it is a true extract from the official records of the bank and that such entries or records are from a computerized system with proper integrity of data, wherein data cannot be manipulated or accessed in an unauthorized manner or is not lost or tamperable due to system failure or such other reasons. Here again, let us reiterate that the law does not state that any computerized print-out even if not signed, constitutes a valid record. But still even many banks of repute (both public sector and private sector) often send out printed letters to customers with the space for signature at the bottom left blank after the line "Yours faithfully" etc and with a remark as Post Script reading: "This is a computer generated letter and hence does not require signature". Such interpretation is grossly misleading and sends a message to public that

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

computer generated reports or letters need not be signed, which is never mentioned anywhere in nor is the import of the ITA or the BBE. The next Act that was amended by the ITA is the Reserve Bank of India Act, 1934. Section 58 of the Act sub-section (2), after clause (p), a clause relating to the regulation of funds transfer through 15 electronic means between banks (i.e. transactions like RTGS and NEFT and other funds transfers) was inserted, to facilitate such electronic funds transfer and ensure legal admissibility of documents and records therein.

Conclusion

India's financial fraud regulations, anchored by the Companies Act, 2013, and strengthened by the new criminal laws BNS and BSA 2023, provide a comprehensive framework to combat fraud. Regulatory bodies, such as the RBI, SEBI, and SFIO, alongside professional standards, ensure robust oversight. Organizations must adopt proactive approaches combining vigorous internal controls, advanced technology, and strong governance frameworks. Given the complexity of modern financial fraud regulations, professionals must stay current with evolving regulatory requirements and emerging fraud detection technologies. The success of this effort requires collaboration between regulators, financial institutions, technology providers, and law enforcement agencies to create a broad defence against financial crimes.

References

1. Atrey, I. (2023). Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. International Journal of Research and Analytical Reviews.
2. Brahmam, K. V., & Muppavaram, A. O. K. (2023). Data Privacy and Cyber Security in India: A Critical Examination of Current Legal Frameworks. Cyber Crime & Cyber Securities in India, 86-94.
3. Bhat TH, Khan AA. Cybercrimes, security and challenges. Int J Adv Res Comput Commun Eng. 2015;4(5).

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

4. Khan R, Taqi M, Afzal A. Deepfakes in finance: Unraveling the threat landscape and detection challenges. In: Navigating the world of deepfake technology. Hershey, PA: IGI Global; 2024. p. 91-120. https://www.irmainternational.org/viewtitle/353615/?isxn=979836 9352984
5. Krishna RA. Unraveling intellectual property: A study on the transformative role of AI and digital innovations. Int J Law Mgmt Human. 2024;7(2):2661.
6. UNODC. (2020). Global Report on Financial Crime and Money Laundering. Vienna: United Nations Office on Drugs and Crime.
7. Houben R, Snyers A. Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. Brussels: European Parliament Study; 2018. https://data.europa.eu/doi/10.2861/280969
8. Kulshrestha P, Gautam R, Singh A, editors. Cybercrime, regulation and security: Contemporary issues and challenges. Delhi: Libertatem Media Pvt Ltd; 2022 Aug 30. doi.org/10.55662/CCRSbook.2022
9. Aidoo S, AML ID. Regulatory Frameworks for Combating Financial Crime in Emerging Markets. 2025. https://www.researchgate.net/profile/FarinuHamzah/publication/393091275_Regulatory_Fram eworks_for_Combating_Financial_Crime_in_Emerging_Markets/links/685ebebfe9b6c13c89e4d7ac/Reg ulatory-Frameworks-for-Combating-FinancialCrime-in-Emerging-Markets.pdf
10. Thomas TA. Understanding digital money as a new modus of money laundering: Legal introspection in India. DNLU Stud Law J. 2023; 2:46. https://dnluslj.in/understanding-digital-money-asa-new-modus-of-money-laundering-legalintrospection-in-india/
11. Ferri C. New approaches to old problems? Thinking about a new design of the AML/CFT strategy. arXiv preprint. 2024; arXiv:2405.18517
12. Gulyamov S, Raimberdiyev S. Personal data protection as a tool to fight cyber corruption. Int J Law Policy. 2023;1(7):1-32. https://doi.org/10.59022/ijlp.119
13. Prakash, P., Girdhar, S., & Jose, A. (2023). Indian Cyber Act: Lacunae and Recommendations. Issue 6 Int'l JL Mgmt. & Human., 6, 2944.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20684913

14. Halder, D. (2015). A Retrospective Analysis of Section 66 a: Could Section 66 a of the Information Technology Act Be Reconsidered for Regulating'Bad Talk'in the Internet?. Halder Debarati," A Retrospective Analysis of Section, 66, 98-128.

15. Singh, A., & Chauhan, P. S. (2023). Navigating Digital Legislation: A Comprehensive Analysis of India's It Act And Emerging Cyber Security Challenges. Computer Integrated Manufacturing Systems, 29(4), 297-321.