ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC - NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

A brief analysis of law relating to cyber fraud in India and international perspective

Authored by - Sudhakar Rolan
PhD Research Scholar
Department of Law
University of Rajasthan Jaipur

Introduction

Cyber fraud is a type of criminal activity that involves the use of technology, such as computers, smartphones, and the internet, to commit fraudulent activities. Cyber fraud is a broad term that encompasses a wide range of activities, including but not limited to:

Phishing: This is a form of cyber fraud that involves sending fraudulent emails, text messages, or other electronic communications that are designed to trick individuals into revealing sensitive information such as passwords or credit card numbers.

Identity theft: This involves stealing someone's personal information, such as their name, date of birth, and Social Security number, and using it to open fraudulent accounts or make unauthorized purchases.

Online scams: These are fraudulent schemes that are designed to trick individuals into paying money or providing personal information under false pretenses. Examples of online scams include lottery scams, job scams, and romance scams.

PlMalware: Malware is software that is designed to harm or disrupt computer systems. Cyber criminals may use malware to gain unauthorized access to computer systems, steal sensitive information, or encrypt data and demand a ransom for its release.

Business email compromise (BEC): BEC involves impersonating a legitimate company or

ISSN: 2582-6433

business partner to deceive individuals into transferring money or providing sensitive information.

Cyber fraud is a growing problem globally, with criminals constantly finding new ways to exploit technology for their own gain. It can have serious consequences for individuals, businesses, and society as a whole, including financial loss, identity theft, and reputational damage.

Cyber fraud cases in India:

There have been several high-profile cyber fraud cases in India over the years. Some of the notable cases and their trials are:

PNB Fraud Case: In 2018, it was discovered that a fraudulent transaction of over Rs 13,000 crore had taken place at Punjab National Bank (PNB), one of India's largest banks. The fraud involved the issuance of fake letters of credit to companies owned by Nirav Modi and Mehul Choksi. Several people, including bank employees and the accused businessmen, were arrested and are currently on trial.

Mphasis Case: In 2021, it was reported that a former employee of Mphasis, an IT services company, had committed a fraud of over Rs 10 crore by transferring funds from the company's accounts to his personal accounts. The accused was arrested and is currently on trial.

Unocoin Case: In 2018, the co-founders of Unocoin, a bitcoin exchange company, were arrested for installing a bitcoin ATM kiosk in Bengaluru without obtaining the necessary permissions. They were charged with various offenses, including cheating and forgery, and were eventually released on bail.

Syndicate Bank Case: In 2016, the Central Bureau of Investigation (CBI) arrested several people, including the chairman of Syndicate Bank, for allegedly accepting bribes to extend loans to companies that were not creditworthy. The accused are currently on trial.

The trials of these cases are ongoing, and the outcomes are yet to be determined. The Indian legal system has various laws and provisions to deal with cyber fraud, including the

ISSN: 2582-6433

Information Technology Act, 2000, and the Indian Penal Code, which provide for penalties and punishments for offenses related to cyber fraud. The authorities are working to strengthen their capacity to investigate and prosecute cyber fraud and to promote greater awareness among individuals and organizations to prevent such incidents.

Cyber fraud laws in India:

Cyber fraud is a serious offense in India and is covered under various laws and regulations. Some of the key laws and regulations related to cyber fraud in India are:

Information Technology Act, 2000: This is the primary law governing cybercrime in India. The act defines various cyber offenses, including unauthorized access, hacking, cyberstalking, phishing, identity theft, etc. The act also provides for penalties and punishments for such offenses.

Indian Penal Code, 1860: The IPC also provides for provisions related to cybercrime. Sections 419 to 424 of the IPC deal with offenses related to cheating, impersonation, and fraud. Sections 463 to 471 of the IPC deal with offenses related to forgery, counterfeiting, and using forged documents.

Reserve Bank of India (RBI) Guidelines: The RBI has issued various guidelines related to cyber fraud prevention for banks and financial institutions. These guidelines cover various aspects of cybersecurity, including information security, risk management, fraud prevention, and customer education.

Prevention of Money Laundering Act, 2002: This act provides for the prevention, detection, and punishment of money laundering offenses, which are often linked to cyber fraud.

Indian Cyber Crime Coordination Centre (I4C): The I4C was set up in 2018 to combat cybercrime in India. It is a central agency responsible for coordinating and strengthening the efforts of law enforcement agencies, intelligence agencies, and other stakeholders to prevent and investigate cybercrime.

National Cyber Security Policy, 2013: This policy outlines the government's vision and

ISSN: 2582-6433

strategy for securing cyberspace in India. It covers various aspects of cybersecurity, including legal and regulatory frameworks, information sharing, capacity building, and international cooperation.

These laws and regulations provide a comprehensive framework for preventing and combating cyber fraud in India. However, the effectiveness of these laws depends on their implementation and enforcement by the authorities.

Trial procedure of Cyber fraud cases in India:

The trial procedure for cyber fraud cases in India is governed by the Code of Criminal Procedure, 1973, and the Information Technology (IT) Act, 2000. The following is the general trial procedure for cyber fraud cases in India:

Registration of FIR: A cyber fraud case begins with the registration of a First Information Report (FIR) with the police. The FIR sets out the details of the alleged cybercrime, the complainant, and the accused.

Investigation: The police will investigate the case and collect evidence, including digital evidence such as emails, chat logs, and server logs.

Charge sheet: Once the investigation is complete, the police will submit a charge sheet to the court, which sets out the evidence against the accused and the charges filed against them.

Framing of charges: The court will examine the charge sheet and determine if there is sufficient evidence to proceed with the trial. If so, the court will frame charges against the accused.

Trial: The trial will be conducted in accordance with the Code of Criminal Procedure, 1973, and the IT Act, 2000. The prosecution will present evidence to prove the charges against the accused, and the accused will have the opportunity to present their defense.

Verdict: After the trial is complete, the court will deliver its verdict. If the accused is found guilty, the court will pronounce the sentence.

It is important to note that cyber fraud cases involve digital evidence, which requires specialized knowledge and expertise. The courts may appoint a technical expert to assist in the

ISSN: 2582-6433

investigation and trial of cyber fraud cases. Additionally, the IT Act, 2000, provides for certain procedural safeguards, such as the requirement of a warrant for search and seizure of electronic devices, to protect the privacy and rights of individuals.

International cyber fraud investigation agencies:

There are several agencies at the national and international level that are responsible for investigating cyber fraud. Some of the key agencies are:

Federal Bureau of Investigation (FBI): The FBI is the primary law enforcement agency of the United States federal government, responsible for investigating federal crimes, including cybercrime.

National Cyber Investigative Joint Task Force (NCIJTF): The NCIJTF is a multi-agency task force within the United States government that coordinates the investigation and response to cyber threats.

National Crime Agency (NCA): The NCA is a law enforcement agency in the United Kingdom responsible for investigating serious and organized crime, including cybercrime.

Australian Cyber Security Centre (ACSC): The ACSC is a government agency in Australia responsible for coordinating the government's response to cybersecurity threats, including cybercrime.

European Cybercrime Centre (EC3): The EC3 is a center within Europol that provides operational support to member states in investigating and preventing cybercrime in Europe.

Cybercrime Investigation Cell (CIC): The CIC is a specialized unit within the Indian police force responsible for investigating cybercrime in India.

Cyber Crime Unit (CCU): The CCU is a specialized unit within the Royal Canadian Mounted Police (RCMP) responsible for investigating cybercrime in Canada.

These agencies, along with various other national and international agencies, play a critical role in investigating and prosecuting cyber fraud. They use a range of techniques and tools,

ISSN: 2582-6433

including forensic analysis, data mining, and international cooperation, to identify and apprehend cybercriminals and disrupt their operations.

International perspective of law relating to Cyber fraud:

Cyber fraud is a global problem and is covered under various laws and regulations in different countries. Some of the key international laws and regulations related to cyber fraud are:

Council of Europe Convention on Cybercrime: This is a multilateral treaty that provides a framework for international cooperation in the investigation and prosecution of cybercrime. The convention covers various cyber offenses, including illegal access, interception of data, and computer-related fraud.

United States Computer Fraud and Abuse Act (CFAA): This act prohibits various computer-related offenses, including unauthorized access, hacking, and computer-related fraud. It also provides for penalties and punishments for such offences.

European Union General Data Protection Regulation (GDPR): The GDPR is a regulation that governs the protection of personal data of EU citizens. It imposes strict requirements on organizations that process personal data and provides for penalties and fines for non-compliance.

United Nations Convention against Transnational Organized Crime: This convention provides a framework for international cooperation in the prevention and prosecution of transnational organized crime, which often involves cyber fraud.

International Association of Financial Crimes Investigators (IAFCI): The IAFCI is a global organization that promotes the prevention, detection, and investigation of financial crimes, including cyber fraud.

These laws and regulations, along with various other international initiatives, provide a comprehensive framework for preventing and combating cyber fraud at the global level. However, the effectiveness of these laws depends on their implementation and enforcement by the authorities in different countries. Therefore, international cooperation and coordination are

ISSN: 2582-6433

crucial to addressing the global problem of cyber fraud.

International organisations on cyber fraud crimes:

There are several international organizations that are working to combat cyber fraud and other forms of cybercrime. Some of the key organizations are:

Interpol: Interpol is the world's largest international police organization, with 194 member countries. It coordinates international police cooperation and provides a range of services, including support for investigations related to cybercrime.

United Nations Office on Drugs and Crime (UNODC): The UNODC is a global organization that works to combat transnational organized crime, including cybercrime. It provides technical assistance, capacity building, and coordination support to member states.

European Cybercrime Centre (EC3): The EC3 is a center within Europol that works to combat cybercrime in Europe. It provides operational support to member states, conducts research, and facilitates international cooperation.

International Association of Financial Crimes Investigators (IAFCI): The IAFCI is a global organization that promotes the prevention, detection, and investigation of financial crimes, including cyber fraud.

Asia Pacific Economic Cooperation (APEC) Cybersecurity Working Group: The APEC Cybersecurity Working Group is a forum for member economies to collaborate on cybersecurity policy and capacity building. It aims to promote cybersecurity cooperation and information sharing among member economies.

Organisation for Economic Co-operation and Development (OECD) Working Party on Security and Privacy in the Digital Economy: The OECD Working Party on Security and Privacy in the Digital Economy provides a forum for member countries to exchange information and best practices on cybersecurity policy and capacity building.

These organizations, along with various other international initiatives, are working to strengthen the global response to cyber fraud and other forms of cybercrime. Their efforts are crucial to addressing the complex and evolving nature of cyber threats and to ensuring the

ISSN: 2582-6433

safety and security of the digital economy.

Conclusion:

Cyber fraud crimes are becoming increasingly prevalent in today's digital age. As more and more businesses and individuals rely on technology to store and process sensitive information, cybercriminals have become adept at exploiting vulnerabilities in online systems to steal data and money.

To combat cyber fraud crimes effectively, it is crucial to have strong laws and regulations in place that can deter criminal behavior, provide avenues for investigation and prosecution, and ensure that victims are adequately protected.

Effective laws and regulations should cover a range of cyber fraud crimes, including identity theft, phishing, ransomware attacks, and other forms of cybercrime. They should also specify the penalties for committing these crimes, which should be severe enough to deter potential offenders.

Additionally, it is important to have regulatory bodies that can monitor and enforce compliance with these laws and regulations. These bodies should have the power to investigate suspected cyber fraud crimes and impose penalties on those found guilty of violating the law. the need for effective laws and regulations to control cyber fraud crimes is essential to protect individuals and businesses from the devastating effects of cybercrime. Only through strong laws and regulations, enforced by dedicated regulatory bodies, can we hope to combat the growing threat of cyber fraud crimes.

Reference:

Dr. Vishwanath Paranjape, Legal Dimensions of Cyber Crimes and Preventive Laws with Special
Reference to India, Central Law Agency Publication, Allahabad, 2010
L. J. Janczewski and A. M. Colarik, Cyber Warfare And Cyber Terrorism, Information Science Reference, 2008.

ISSN: 2582-6433

M. J. Warren, "Terrorism and the Internet," Cyber Warfare And Cyber Terrorism, Information Science Reference, 2008

Tikk & R. Oorn, Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism, in Responses to Cyber Terrorism (Centre Of Excellence Defence Against Terrorism, ed. 2008)

M. Bozdemir, "What Is Terror and Terrorism?," School of Political Sciences Press and Publication College, 1981.

K. Knop, "Institutionalization of a web-focused, multinational counter-terrorism campaign – Building a collective open source intelligent system, A discussion paper," Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism, Ankara, Turkey (Ed.) IOS Press, 2008

M. Gercke et al, Terrorist Use of the Internet and Legal Response, Freedom from Fear, Aug 2011, available at http://www.freedomfromfearmagazine.org/index.php?option¼com_content&view¼article&id¼306:terrorist-use-of-the-Internet-andlegalesponse&catid

T. Oba, "Cyberterrorism seen as future threat," Computer Crime Research Centre Tech. Report, April 2004, http://www.crime-research.org/news/2003/04/Mess0103.html

Z. Sütalan, "Current and future trends in terrorism," COE-DAT Newsletter vol.3 issue.16 p.37-49, July-September 2010.

N. Muddaraju and Ramesh, "Cyber Crimes: Need an Effective Law", pp. 227-31, Criminal Law Journal, 2009 Aug