Vol. 11, Issue: 09, September: 2023
ISSN:(P) 2347-5404 ISSN:(O)2320 771X

Emerging Trends in Technology and its Impact on Law, Criminal Justice, and Public Policy: Financial Frauds in Cyber Space

PRIYADHARSHINI J.
Department of Criminology,
University of Madras.
Centre of Excellence in Digital Forensics.

Abstract:
Money is the most integral commodity for every human to survive. In the modern era, with the growth and dependency on cyber space for every aspect, monetary transactions are no exemption. This paper will propose the vulnerability and apparent ways of financial frauds that may befall upon any person who relies on cyber space. The characteristics of Routine Activity Theory as connoted by Cohen and Felson (1979) is that a criminal event requires a convergence in space and time of a likely offender, a suitable target, and the absence of capable guardian, is very much a criterion for such frauds. The methodological approach would examine the types of financial frauds, the governing laws, and the possible prosecution, including the bay of jurisdiction of the land. The findings will reflect the most conceivable and potential conducts of cyber - related financial frauds, what could be the possible ways to mitigate victimization through such frauds, the potential legal remedies and, possibly the enhancement of regulations by the law makers to assist the Criminal Justice System Agencies to adapt to alleviate the various reigning and evolving forms of financial frauds in the digital space. The result of the paper may bring light to matters of cyber space related financial frauds and furthermore financial frauds which are contemporary but unjustified to be considered as a "fraud".

Keywords: *Routine Activity Theory, Types of Financial frauds, Victimization, Vulnerability, Regulations, Digital Space*

1. Introduction

Money is the most essential commodity which is pivotal for any person to sustain their living. What started as barter where commodities connoted as financial transactions evolved to currency as a mode of transaction. In the light of the 20st century where telegraph business had started, the first long distance customer to customer money transfer took place. In 1974, a British woman ordered groceries through videotex on her TV but paid in cash. The revolution of payment through online or the internet was paved when Tim Berners – Lee invented the World Wide Web (WWW). In 2009, Venmo was launched as a platform for non – physical transfer of money with the use of internet. This revolution followed other technology giants to transfer their own online payment platforms such as Apple pay, Google pay, PayPal, etc.

Industrial Credit and Investment Corporation of India (ICICI), using electronic banking at its branches, launched online banking services in India in 1996. Banks including Citi, IndusInd, and Housing Development Finance Corporation Limited (HDFC) offered online banking services later in 1999. As more banks introduced net banking services in India, the tendency kept expanding. The era of digital transactions in India officially began at this point when several new banks began to provide services to customers.[1] The National Payments Corporation of India (NPCI) began operations in 2008. It was established by the Indian Banks' Association (IBA) and the Reserve Bank of India (RBI) to build a strong payment and settlement infrastructure in India. Since then, it has introduced several products, including the BHIM (Bharath Interface for Money), Aadhaar Enabled Payments System, and Cheque Transaction System. Government of India has perceived 10 different types of digital payments methods, they include:[2]

1.Banking card - The Central Bank of India introduced the Banking Card, the country's first credit card, in 1980. Prior to the introduction of MasterCard in 1993, numerous PSU banks began providing credit cards.

2.Unstructured Supplementary Service Data (USSD) - In 2016, the USSD functionality was introduced. The ability to use mobile banking without a smartphone or an Internet connection is provided by this function.

3.Aadhaar Enabled Payment Systems (AEPS) - Using the business correspondent of any bank and Aadhaar identification, this bank-led strategy enables online interoperable financial inclusion transactions at the point of sale (PoS).

4.Unified Payments Interface (UPI) - UPI, which was created by NPCI (National Payments Corporation of India) in 2016, makes peer-to-peer and person-to-merchant transactions easier. Any consumer holding any bank account can send and receive money using a UPI-based app owing to its interoperable payment system. The system enables users to instantly initiate financial transfers and submit collect requests around-the-clock, every day of the year, by linking several bank accounts to a UPI app on the smartphone. UPI's key benefit is that it makes it possible for users to send money without a bank account or IFSC (Indian Financial System Code) number. A Virtual Payment Address (VPA) is all that is required.

5.Mobile Wallet - A mobile wallet is a particular kind of app-based virtual wallet service. To enable secure payments, the digital or mobile wallet holds bank account, debit/credit card, or bank account information in an encrypted way. A mobile wallet can also be topped up with cash, which can then be used to make payments and make purchases. It was no longer necessary to utilise credit or debit cards, or to keep track of the Card Verification Value (CVV) or 4-digit pin.

6.Bank Pre-Paid Card - A prepaid card is a kind of payment mechanism where you load money onto prior purchasing items. The customer's bank account may not be connected to the type of card. However, a bank-issued debit card is connected to the customer's bank account. Users with pre-paid cards are allowed to make purchases with the cash still on their cards, strictly adhering to the maxim "Pay Now, Use Later."

7.Point of Sale - A merchant establishment (ME) can use a Point of Sale (PoS) as a technological tool to conduct cashless sales of goods and services to consumers. PoS terminals have historically been understood to be those that are deployed at all stores where customers use credit/debit cards to make transactions. A handheld gadget is typically used to read bank cards. However, as a result of digitization, the reach of PoS is growing and this service is now accessible via internet browsers and mobile platforms as well. PoS terminals come in a variety of forms, including physical, mobile, and virtual. The ones that are stored at shops and retailers are the physical PoS terminals.

8.Internet Banking - Online banking transactions are referred to as internet banking. Many different services, including money transfers, opening new fixed or periodic deposits, cancelling accounts, etc., may fall under this category. E-banking or virtual banking are other names for internet banking. For National Electronics Fund Transfer (NEFT), Real Time Gross Settlement (RTGS), or Immediate Payment Services (IMPS) online fund transfers, internet banking is widely utilized. Through their websites, banks provide customers with a variety of financial services, and those customers can access their accounts by entering a username and password. Internet banking services can be used at any time

[1] Upasana Ghosh, 2021. "Online Financial Frauds and Cyber Laws in India -An Analysis," Working papers 2021 38-09, Voice of Research.

[2] Cashless India, Government of India (http://cashlessindia.gov.in/digital_payment_methods.html)

and on any day of the year, unlike visiting a physical bank, which has time constraints. The potential for online banking services is enormous.
9.Mobile Banking - The process of doing banking or financial transactions using a smartphone is referred to as mobile banking. With the development of numerous mobile wallets, digital payment apps, and other services like the UPI, the reach of mobile banking is only growing. Customers can download the applications from any number of banks to conduct banking transactions at the touch of a button. The phrase "mobile banking" is used to refer to a broad range of services that fall within this category.
10.Micro ATMs - Customers can access financial services using micro-ATMs. Micro ATMs can be facilitated by business partners, who may be local business owners, to carry out quick transactions. Through this gadget, you can transfer money using fingerprint authentication from a bank account that is connected to the Aadhaar. This Micro ATM offers several important services, such as withdrawal, deposit, money transfer, and balance enquiry.

Cyber payments systems provide for faster, simpler, and more convenient transactions than traditional banking methods, which require visiting a branch. Digital transactions are more affordable than conventional payment methods. and are better because people may access several promotions and bonuses for carrying out digital transactions. Digital transactions give a clear trail of the whole transaction, making it easier to track payments. To facilitate the growth of internet banking in India, both the Indian Government and the Reserve Bank of India implemented a number of steps. The Government of India passed the Information Technology Act, 2000, which gave legal status to electronic transactions and included rules for dealing with e-commerce, with effect from October 17, 2000.[3] The act was later amended in 2008 and the Information Technology (Amendment) Act, 2008 has been applied in places of cyber related offences along with other special laws and penal laws of the country.

With the growth of technology and the acquaintance of all the electronic devices with the internet, there is also a bane. Perpetrators in the cyber realm are imperceptible and are cryptic offenders. Unlike conventional crimes, mapping using digital evidence can take a longer time due to the vantage point that the offender can be present anywhere around the globe and the Modus Operandi is challenging to identify due to the malleable execution of the crime. The Reserve Bank of India has issued several guidelines to the financial institutions to prevent any loss occurring through internet banking and financial services. The Banking Regulation Act of 1949 does not specifically address banking frauds, but the provisions of this Act make it easier to comprehend how the banking industry functions and the causes of widespread fraud.[4]

2. Financial frauds in cyber space

With everything available at the stroke of a button, including online shopping, restaurant ordering, and payment processing, better technology, internet usage, and digitalization have made life simpler for everyone. Similar to the adage "Every coin has two sides," digitalization has facilitated for numerous frauds, including identity theft, data breaches, online scams, email scams, and charity scams.

The paper on the topic “*Emerging Trends in Technology and its Impact on Law, Criminal Justice, and Public Policy: Financial Frauds in Cyber Space”* shall highlight the trend of the financial frauds that exist in the millennium and its relevance with the law and the Criminal Justice System which can help to identify the pace at which the law keeps up with the cyber financial frauds as like of conventional crimes and the effectual ways of mitigation through considerable, viable and tactical techniques.

The following chapter will contain the literature review relating to the current study.

[3] Chandrawati NIrala, Dr, BB. Pandey, ‘Evolution of e-banking in India- An Empirical Study

[4] Upasana Ghosh, 2021. "Online Financial Frauds and Cyber Laws in India -An Analysis," Working papers 2021 38-09, Voice of Research.

3. Review of literature

This chapter shall include literatures, surveys and reports pertaining to the financial frauds in cyber space. It shall include:

1.Literatures relating to what is a cyber space and the aspects of a cyber network and internet.
2.Literatures relating to what are the various types of cyber financial frauds.
3.Literatures relating to the Indian laws tackling the cyber financial frauds.

Berry et al., (2009) in their study mentioned that one of the most significant inventions of the twenty-first century that has significantly impacted our lives is the Internet. Today, the internet has eliminated all barriers and revolutionised how we interact with one another, play games, work, shop, make friends, watch movies, order food, pay bills, and wish people happy birthdays and anniversaries.[5] Security is essential in the digital age because it permeates every aspect of our daily lives, both public and private. Without security, everything in the world will crumble.

Cybersecurity is the first thing that comes to mind when we encounter a fraud. Our worry for online data security has grown significantly. In recent years, the number of linked devices has rapidly increased; by 2020, that number will have surpassed 50 billion. (Dawson, J and Thomson, R., 2018). [6] Computer is used as a tool for fraud since it has a large amount of data recorded, including confidential data and information, and it is simple to access to steal data using covertly implanted key loggers and logic bombs. If there is no adequate backup, the data gathered is exploited and destroyed after usage, which can also lead to the loss of evidence and proof of facts. Mobile devices are also employed in fraud schemes (Siddique, I and Rehman, J. 2011).[7]

Both a useful conceptual framework for the investigation of such crimes and a widely accepted definition of the phrase "financial crime" are absent. Developing a more in-depth grasp of the categories of legality and illegality, as well as the relationship between the dimensions of (formal) legality and (social) legitimacy, is a crucial first step in conceptualising financial crimes. (Mayntz 2016)[8]

The Routine Activity Theory’s core principles clarify that crimes happen when conditions that are conducive to crime come together to create criminal possibilities. The routine activity theory states that when motivated offenders come across eligible targets without capable guardianship, they will take advantage of opportunities. In the framework of routine activity theory, cybercrimes rely on computer networks to link motivated offenders with potential victims in the absence of capable supervision. The cyberlifestyle-routine activities theory contends that by viewing their interaction as "delayed" in time, motivated offenders and appropriate targets can be brought together while being separated in time (Steinmetz, K.F., & Nobles, M.R., 2017).[9]

To identify three forms of crime—bank-related fraud schemes (54%), fake lottery scams (22%), and false delivery services (14%), researchers Isacenkova et al., (2013); Kigerl (2009) used frequencies in

[5] Barry M. Leiner et. al., “A Brief History of the Internet,” ACM SIGCOMM Computer Communication Review, Volume 39, Number 5, October 2009

[6] Dawson, J. and Thomson, R., “The future cybersecurity workforce: Going beyond technical skills for successful cyber performance”, Frontiers in Psychology, 9(JUN), pp. 1–12, 2018.

[7] Siddique, I. & Rehman, S. (2011) "Impact of Electronic Crime in Indian Banking Sector-An Overview, “International Journal of Business & Information Technology”.

[8] Mayntz, Renate, 2016: *Illegal Markets: Boundaries and Interfaces between Legality and Illegality.* MPIfG Discussion Paper 16/4. Cologne: Max Planck Institute for the Study of Societies

[9] Steinmetz, K.F., & Nobles, M.R. (2017). Technocrime and Criminological Theory (1st ed.). Routledge. https://doi.org/10.4324/9781315117249

email language distribution data. [10] [11] Whitty (2013) lists three different ways people make money, including creating phoney identities and personas to disguise their ethnicity. [12]

Suleiman (2019) discusses the use of spam email as an infiltration strategy in Nigerian letter fraud. He did not stress or add to the narrative with his study. Numerous studies explain the geographic distribution of fraud and scams after the distribution of bulk campaign emails that raise the danger of becoming a victim to financial fraud.[13]

Bitcoin scams by hacking into digital wallets has become simple. Scammers are using it to their advantage. This new technology is being used by cybercriminals to steal valuable data from victims (M. Vasek and T. Moore, 2015). [14]

Scams using credit cards or bank loans prey on consumers by asking them to guarantee enormous sums of money that the bank has already preapproved. Scammers ensnared victims with this offer and demanded payment in exchange for access to the authorised enormous sum of money. Victimized are those who depend on them and pay the required costs (Drake, C.E., Oliver, J.J., & Koontz, E.,2004).[15] The IT Act 2000 defines cybercrimes as bailable offences by default; they are only not bailable when they are connected to The Indian Penal Code, 1860 offences, giving the criminal plenty of opportunity to delete evidence after being released on bail. The rise in online financial frauds emphasises the necessity to establish a more comprehensive regulatory framework to safeguard our technical independence. Additionally, the Information Technology Act of 2000 makes no mention of data security or privacy. In order to prevent data breaches while making a digital payment, India has to have current and specialised legislation on digital money transactions. Because there is no formal regulatory framework, scammers have the opportunity to steal personal information. (Ghosh, U., 2021)[16]

The next Chapter shall lay out the Research Methodology adopted for the current study.

4. Resrarch Methodology

The paper is based as a non – empirical study. Both primary and secondary sources were used to get the non-empirical data. Referrals to primary sources include statutes, laws, and case studies, whereas references to secondary sources include journals, periodicals, and websites.

5. Findings and discussions.

This Chapter shall include the findings based on the primary and secondary sources and the deliberations on such findings.

1)The Department of Justice (DOJ) of the United States categorises cybercrime into three groups:[17]

1. Criminal acts that target electronic devices
2. Criminal acts in which a computer is a weapon

[10] Isacenkova, J., Thonnard, O., Costin, A., Balzarotti, D., & Francillon, A. (2013). Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations. *2013 IEEE Security and Privacy Workshops, Security and Privacy Workshops (SPW), 2013 IEEE, Security and Privacy Workshops, IEEE Symposium On*, 143–150. https://doi.org/10.1109/SPW.2013.15

[11] Kigerl, A. C. (2009). CAN SPAM Act: An Empirical analysis. International Journal of Cyber Criminology, 3(2), 566–589.

[12] Whitty, M.T. 2013. The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam. British Journal of Criminology 53 (4): 665–684.

[13] Suleiman, A. O. (2019). The Impulsive Upsurge of Yahoo-Yahoo in the 21st Century in Nigeria: Islamic Perspective. African Journal of Criminology & Justice Studies, *[s. l.]*, v. 12, n. 1, p. 91–104, 2019.

[14] M. Vasek and T. Moore, “There’ s No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams,” 2015.

[15] Drake, C.E., Oliver, J.J., & Koontz, E. (2004). Anatomy of a Phishing Email. *CEAS.*

[16] Upasana Ghosh 2021, Online Financial Frauds and Cyber Laws in India -An Analysis

[17] Kim, C. Newberger, B. Shack, B. (2012) *American Criminal Law Review* Volume: 49 Issue: 2 Dated: Spring 2012 Pages: 443-488

3. Criminal offences where a computer is employed as an auxiliary.

2)Moher, D (2009) in their study proposed a wall matrix for cybercrimes which is mentioned below:[18]

CRIME TYPE (OPPERTUNITIES)	DEVICE AS A TARGET	DEVICE AS A WEAPON	DEVICE AS AN AUXILIARY
CYBER – ASSISTED	Telecom network	Financial Frauds	Cyber – stalking
CYBER – ENABMLED	Viruses and Malware	Identity theft	Hate speech
CYBER - DEPENDENT	Denial of Service	Phishing, Skimming	Online grooming and pornography

3)European Union Agency for Network and Information Security (ENISA), 2018 in their study stated that:[19]

a) The financial industry reports losses in the billions each year. Individuals lost £10 billion in 2016, which amounts to around 2 million cyber-related fraud instances, according to the UK National Audit Office. By 2020, online fraud may have surpassed plastic fraud if current trends continue.
b) The Society for Worldwide Interbank Financial Telecommunications (SWIFT) procedures came under examination from SWIFT members in 2015 and 2016 because they gave users of the end equipment too much discretion, which was considered a weakness. One of the greatest cyber-attacks that cost 81 million dollars was allegedly carried out by a central bank in Asia that exploited the SWIFT network.
c) Early in August 2018, a different attack resulted in the theft of US $13.5 million from India's Cosmos Bank. It was an attack that revealed flaws on the defence banks had in place against certain cyberthreats. The bank's infrastructure was the major target of the more sophisticated, carefully thought-out, and meticulously organised attack, which effectively avoided the four main lines of defence. The checks on card number, card status, PIN, and other information were never carried out since the information sent from the payment switch to allow transactions was never transferred to the main banking system. Instead, the malicious proxy used by the attackers to send bogus replies and authorise transactions processed the request.
d) Data that has been stolen or compromised is frequently discovered on the Dark Web, where it is sometimes sold in Dark Web marketplaces alongside unlawful content. Some of the most typical items that may be discovered there include drugs, the most recent exploits, and stolen personal information (credit cards, IDs). The Onion Router (ToR) or the Invisible Internet Project are two examples of the specialised software needed to access the Dark Web, which is a portion of the Internet (I2P). Although there are accusations that Government agencies were able to track and locate persons utilising such services, the objective behind this type of network is that access is anonymous and untraceable.
e) On June 19, 2018, the official journal of the European Union released the 5th Anti-Money Laundering Directive, which modifies the 4th Anti-Money Laundering Directive. By 10 January 2020, the Member States must have implemented this Directive. The updated regulations will now bring cryptocurrency exchanges, digital wallets, and virtual currencies under its oversight. This inclusion is justified by the rise in the usage of cryptocurrencies by criminal groups for money laundering and ransomware (Petya, NotPetya).

[18] David Moher et al. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement". In: Annals of internal medicine 151.4 (2009), pp. 264-269

[19] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/financial-fraud-in-the-digital-space

4)The ability of classic Routine Activity Theory (RAT) features to explain victims in cases of cybercrimes where they appear to have minimal impact is a key concern. Why does the likelihood of being a victim of malware and identity theft not rise with the victims' financial status? These are the only two crimes in which the perpetrator is interested in getting the victims' money. Does the Internet give criminals the means to make money by randomly assaulting as many people as they can, as opposed to concentrating their efforts on those from whom they might be able to obtain substantial amounts of money illegally? In that case, "value" and possibly "visibility" are becoming less significant in the context of financial crimes and are being replaced by "online accessibility." If we are to demonstrate the value of RATs in relation to cybercrimes, as well as their limitations, more research is required to answer these problems. [20]

5)The majority of cyber fraud victims are young, salaried people, who are typically believed to be tech-savvy, according to a survey of cyber and banking scams by HDFC Bank. Social engineering is used to conduct fraud. [21]

1. The scammers' social engineering techniques follow a script of greed, menace, or assistance.
2. It has been noted that frauds take place in broad daylight. Presently, 65 to 70 percent of cybercrimes take place between 7 a.m. and 7 p.m. Contrary to popular belief, frauds do not often occur at odd hours of the night. Additionally, researchers discovered that 80–85 percent of the affected clients fall into the 22–50 age bracket, which is considered to be a tech-savvy age range. Additionally, it was shown that frauds frequently include salaried workers who are thought to be knowledgeable. Additionally, it was discovered that men are the target of frauds more often than women.

6)Data from CERT-In (Indian Computer Emergency Response Team)[22] shows that the first two months of 2022 saw more cybercrimes recorded than the entire year of 2018. The nodal organisation for handling threats to cyber security, CERT-In, works under the Ministry of Information Technology. Since 2018, the number of cybercrime cases has steadily increased. In 2018, India reported 2,08,456 incidents; in 2019, 3,94,499 incidents; in 2020, 11,58,208 instances; in 2021, 14,02,809 cases; and in 2022's first two months, 2,12,485 incidents. According to the CERT - In statistics, cybercrimes surged about seven-fold between 2018 and 2021, and they climbed even more dramatically during the pandemic. According to additional CERT-In data, there were a total of 17,560, 24,768, and 26,121 hacks on Indian websites in 2018, 2019, and 2020, respectively.

7)India had a pretty substantial online fraud experience rate of 69% in the previous year, according to the Microsoft 2021 Global Tech Support Scam Research report:

1. In India, the highest percentage in the world, 31% of people lost money as a result of fraud.
2. Globally, Microsoft Corp. receives about 6,500 complaints from people who have fallen victim to tech support fraud. This is less than the 13,000 reports each month on average from the previous year.
3. In India, 48% of people—three times the global average—were tricked into continuing to commit fraud. 31% of those surveyed kept participating until they ran out of money.
4. In India, 73% of men who dealt with fraudsters anticipated losing money. Customers in India lost an average of ₹15,334 in 2021, while 88 percent were able to partially recover their losses.
5. Millennials (ages 24 to 37) in India were the group most susceptible to such scams in 2021, with financial loss occurring to 58% of those who continued the scam.

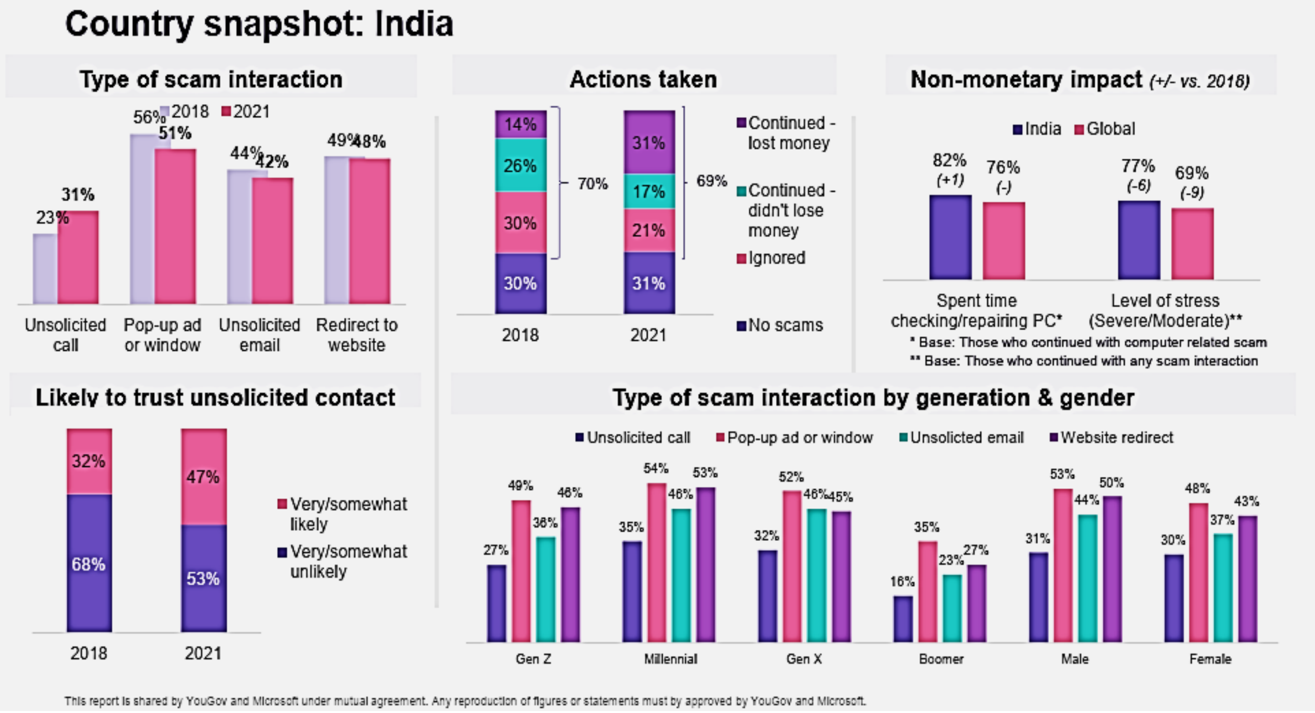
[20] Eric Rutger Leukfeldt & Majid Yar (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis, Deviant Behavior, 37:3, 263-280, DOI: 10.1080/01639625.2015.1012409

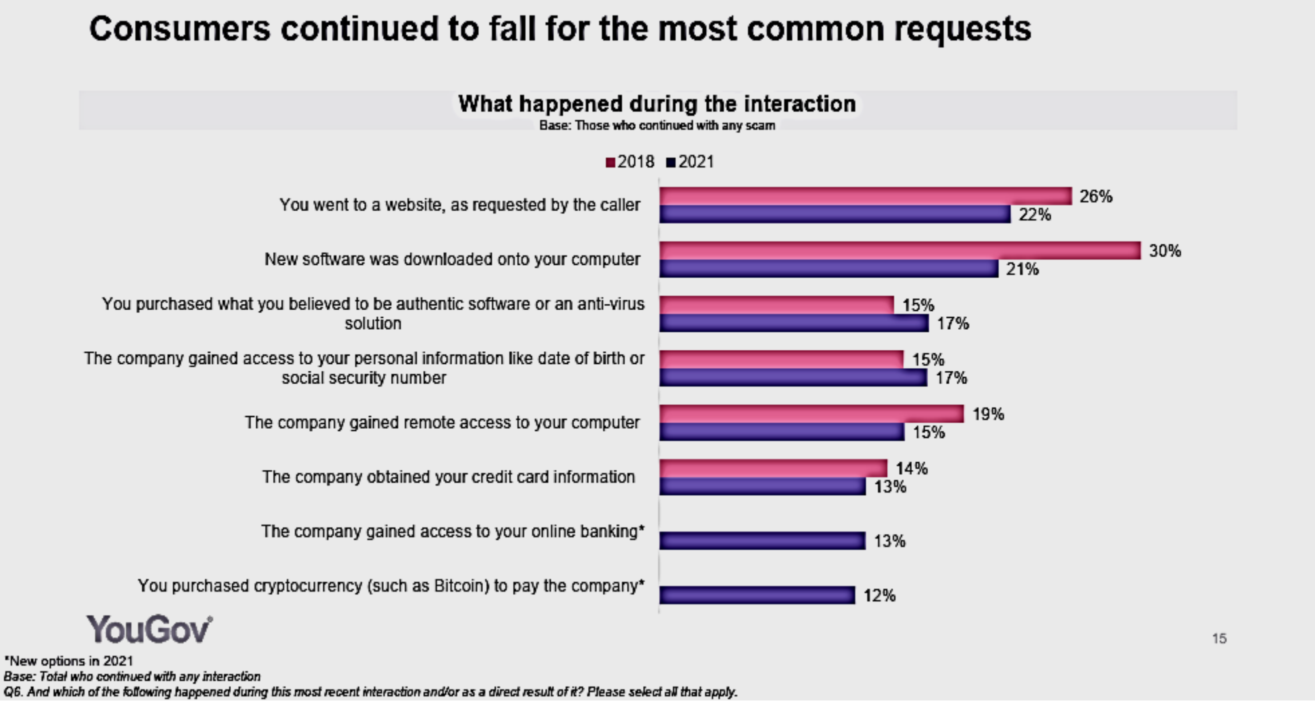
[21] https://www.livemint.com/technology/tech-news/most-people-falling-prey-to-cyber-fraud-attacks-are-in-22-50-years-11645414291787.html

[22] https://zeenews.india.com/technology/two-months-of-2022-saw-more-cyber-crimes-than-entire-2018-why-e-fraud-is-a-ticking-time-bomb-2458733.html

6.The percentage of unsolicited phone calls in India increased from 23% to 31% between 2018 and 2021, and unsolicited phone calls are the fraud type that Indians respond to the most frequently, followed by pop-up ads, website redirects, and anonymous emails.

The following data was sourced as an image from the report which is mentions the statistical data of financial scams and monetary loss incurred by Indians in 2021.[23]





8)Cyber Financial frauds in Indian scenario would include:

1) Telemarketing frauds – Providing fake discounts and free goods to clients to boost sales.
2) Online gambling.

[23] https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf

3) Cybersquatting or Intellectual Property Crimes
4) E – mail spoofing.
5) Forgery.
6) Hacking or unauthorized access to electronic systems.
7) Theft of information which is contained in electronic or digital form.
8) Email bombing – Through this attack, the perpetrators can alter raw data before its processing stage and change back after the computer gas processed it.
9) Salami attack – These are mostly 'revenge-based attacks' as the motive is to make alteration at an insignificant level so that it would be unnoticeable but can cause a sizable damage.
10)Virus or worm attacks.
11)Trojan attacks.
12)Web jacking.
13)Physical theft of computer system or electronic devices.
14)Phishing.
15)Vishing.
16)Spamming.
17)Embezzlement
18)Fake loan provider
19)ATM skimming and Purpose Offer Wrong doings – It is trading off a Point-of-Sale machine or ATM machine and replacing it with a gadget on the keypad that copies its purpose.
20)Credit/Debit card fraud.
21)Online identity theft fraud.
22)Crowd funding fraud.
23)Pharming – redirecting to sites which are fake, and users enter their personal information.
24)Honey trapping – Through online lottery, dating, charity, Ponzi schemes, online auction, money transfer fraud.
25)Sale of items through dark net and unsolicited websites.
26)Ransomware.
27)Blackmail.
28)OTP fraud.
29)UPI fraud.

9)The National Crimes Record Bureau in the Crime in India 2020 statistics mentioned the "Cyber Crime Motives" and the following the motives which pertain to financial frauds:[24]

S. No	Cyber Crime Motive as be Crime in India 2020	Figures (Cases throughout India – States and UTs)
1.	Fraud	30,142
2.	Personal revenge	1470
3.	Anger	822
4.	Extortion	2440
5.	Prank	254
6.	Steal information	62
7.	Others	8814

Note: The cyber-crime motives mentioned in the NCRB does not specifically indicate the above to cyber financial frauds. The contents in the table were made based on the characteristics of a cyber financial fraud.

[24] https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE%209A.3.pdf

10)India reported 50,035 cybercrimes in 2020, 44,546 incidents in 2019, and 27,248 cases in 2018, according to the NCRB's Crime in India - 2020 statistics.[25]

1. 4,047 cases of internet banking fraud, 2,160 cases of ATM fraud, 1,194 cases of credit/debit card fraud, and 1,093 cases of OTP fraud were reported in 2020.
2. Fraud was determined to be the major motive, accounting for 30,142 of the 50,035 cases (60.02 per cent).
3. Karnataka has the highest rate of cybercrime (16.2%), followed by Telangana (13.4%) and Assam (10.1 per cent).

11)Penal provisions in the Information Technology (Amendment) Act, 2008 dealing with Financial Frauds are as follows:[26] [27]

S. No	Section(s) under the Information Technology (Amendment) Act, 2008	Penalty
1.	SECTION 65: **Tampering with computer source documents** Knowingly or intentionally conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
2.	SECTION 66: **Computer Related Offences** Dishonestly, or fraudulently, does any act referred to in section 43([Penalty and compensation] for damage to computer, computer system, etc.	Punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.
3.	SECTION 66A(c): Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages	Punishable with imprisonment for a term which may extend to two three years and with fine.
4.	SECTION 66 C: **Punishment for identity theft** Fraudulently or dishonestly make use of the electronic signature, password, or any other unique identification feature of any other person	Punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
5.	SECTION 66 D: **Punishment for cheating by persionation by using computer resource**	Punished with imprisonment of either description for a term which may extend to three years and shall also be liable to

[25] https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE%209A.1.pdf
[26] India Code, Digital Repository of all central and state acts, https://www.indiacode.nic.in/handle/123456789/1999
[27] https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf

	By means of any communication device or computer resource cheats by personation	fine which may extend to one lakh rupees.
6.	SECTION 74: **Publication for fraudulent purpose** Knowingly creates, publishes, or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose	Punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
7.	SECTION 75: **Act to apply for offence or contraventions committed outside India** •Provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. •Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.	-
8.	SECTION 43: **Penalty and Compensation for damage to computer, computer system**	Pay damages by way of compensation not exceeding one crore rupees to the person so affected

12)Though there are laws to govern the offences in cyber space, there is always an ambiguity between the Information Technology (Amendment) Act, 2008 and the Indian Penal Code, 1860. Though the IT Act 2008 is the supposed sole – governing penal law for cyber-crimes, the IPC, 1860 over – shadows the provisions which causes confusion over the authoritative law. [28] [29] [30]

a) Section 66 of the IT act, 2008 is associated with credit/debit card fraud which is penalised with a sentence of imprisonment of 2 – 3 years with fine upto 5 lakhs. This provision is also read with sections 420 (Cheating and dishonestly inducing delivery of property),467 (Forgery of valuable security, will, etc),468 (Forgery for the purpose of cheating), 471 (Using a genuine forged document or electronic record) of IPC 1860.
b) Phishing is penalised under section 43 of the IT which sanctions 1 crore as payment of damages and sections 379(Punishment for theft) and 420 of IPC, 1860 are read along.
c) Embezzlement has no provision in the IT Act, 2008 but this is treated as criminal breach of trust under IPC 1860, under sections 379, 413 (Habitually dealing with stolen property), 414(Assisting in concealment of stolen property), 420, 467, 468 and 471.
d) Hacking is dealt under section 66 of the IT Act and sections 419 (Punishment for cheating by personation) and 420 of IPC, 1860.
e) Tampering with computer source documents are penalised under section 65 and 66 of their Act, 2008.
f) Planting Virus and other malicious software and Denial of Service attacks are penalised under section 66 of the IT Act, 2008.

[28] http://odishapolicecidcb.gov.in/sites/default/files/Relevant%20Penal%20sections%20Cyber%20Crime.pdf
[29] https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf
[30] https://legislative.gov.in/sites/default/files/A1860-45.pdf

g) E – mail spoofing is penalised under Section 66C of the IT Act, 2008 and sections 465 (Punishment for forgery) and 468 (Forgery for the purpose of cheating) of IPC, 1860.

The penalties of the Indian Penal Code, 1860 have stricter punishments than the IT Act as the penalties under the IT Act, 2008 are bailable, and they are ambiguous with the non – bailable offences of the IPC.

6. The current trend of financial frauds

The Reserve Bank of India has published a booklet to educate banking clients against frauds using digital payments. The brochure outlines the tactics used by con artists and the precautions clients can take before making financial commitments. During the COVID 19 period, there was a substantial increase of cyber crimes where the rate of cyber crimes stood at 3.7% at 2020 as per the Crime in India 2020 statistics.[31]

The booklet by RBI named as "BE – AWARE"[32] contains the emerging existing financial frauds which are to be dealt by Banking and Non – Banking Financial Institutions and its Modus Operandi. They are:

1) Phishing links.
2) Vishing calls
3) Frauds using online sales platform.
4) Frauds due to use of unknown/unverified mobile applications.
5) ATM card skimming.
6) Frauds using screen sharing applications/ Remote access.
7) SIM swap/ SIM cloning.
8) Frauds by compromising credentials through search engines.
9) Scams through QR code scams.
10) Impersonation on social media.
11) Juice jacking (Using charging ports to transfer files/data).
12) Lottery fraud.
13) Online job fraud.
14) Money mules (Innocent victims duped by fraudsters for money laundering or illegal transfer through their bank accounts).
15) Fake advertisements for extending loans by fraudsters.
16) SMS/ E – mail/ Instant message/ Call scams.
17) OTP based frauds.
18) Fake loan websites/ application frauds.
19) Money circulation/Ponzi/ Multi-Level Marketing.
20) Fraudulent loans through forged documents.

7. Significant cases of cyber financial frauds

1. CBI V. ARIF AZIM (SONY SAMBANDH CASE):[33]

NRIs could mail Sony products to their Indian friends and relatives after making an online purchase through the website "www.sony-sambandh.com."

A Sony Colour TV and a cordless phone were ordered for Arif Azim in Noida in May 2002 by someone using the login name Barbara Campa on the website. The order was delivered to Arif Azim after she used his credit card to make the payment. The genuine owner of the card denied making any such purchase, therefore the credit card company notified the business that it was an unlawful payment.

As a result, a complaint was filed with the CBI, and a case was also registered under Sections 418, 419, and 420 of the Indian Penal Code, 1860.

[31] https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE%209A.1.pdf

[32] https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf

[33] [(2008) 105 DRJ 721: (2008) 150 DLT 769]

This was a significant case in the history of cyber law because it showed that the Indian Penal Code, 1860, can be a reliable legislative act to rely on when the IT Act is not sufficient.

2. PUNE CITIBANK MPHASIS CALL CENTER FRAUD: [34]

Facts: In 2005, fraudulent internet transfers totalling US $3,50,000 were made from the Citibank accounts of four US customers to a select number of phoney accounts. In the belief that they would be a helping hand to those customers in dealing with challenging circumstances, the personnel won their trust and collected their PINs. Instead of breaking through firewalls or decrypting encrypted software, they found weaknesses in the Mphasis system.

Decision: The Court noted that the defendants in this case are former MphasiS contact centre employees. Every time an employee enters or exits, they are examined. It is obvious that the workers must have committed the figures to memory. SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, provided the service that was utilised to transmit the cash. Unauthorized access to the victims' electronic accounts was used to commit the crime. As a result, this case is considered a "cyber-crime." The IT Act is sufficiently wide to cover these aspects of criminal behaviour, and any IPC offence involving the use of electronic documents can be treated on a same footing with offences involving written materials.

The court determined that because of the type of unlawful access required to commit transactions, section 43(a) of the IT Act, 2000 is applicable. Additionally, the defendants were charged with violating Sections 66 of the IT Act of 2000, 420 (which refers to cheating), 465, 467, and 471 of the Indian Penal Code of 1860.

3. POONA AUTO ANILLARIES PVT. LTD., PUNE VERSUS PUNJAB NATIONAL BANK, HO NEW DELHI & OTHERS: [35]

Rajesh Aggarwal, the IT secretary for Maharashtra, had ordered PNB to pay the complainant Manmohan Singh Matharu, the managing director of the Pune-based company Poona Auto Ancillaries, Rs. 45 lakhs in 2013, one of the largest settlements awarded in a legal resolution of a cyber-crime issue. After Matharu clicked a link in a phishing email, a fraudster transferred Rs 80.10 lakh from Matharu's account at PNB in Pune. Although the Bank was found responsible for failing to properly screen for fraud accounts formed in an attempt to mislead the complainant, the complainant was urged to share the culpability because he reacted to the phishing email. This was based on Section 43 of IT Act, 2008 – to award compensation for damages to computer or computer system.

4. GENERAL PRECAUTIONS BY RBI TO PREVENT VICTIMIZATION THROUGH CYBER FINANCIAL FRAUDS:

The Reserve bank of India has always provided guidelines time to time based on the increasing trends of cyber crime in general. The Be-Aware booklet[36] of RBI has mentioned general guidelines to be followed by the people to avoid being financially victimized through cyber space, which are summarised below:

1) Be cautious of pop-ups that seem strange when you are exploring the internet.
2) Before conducting any online transactions, always look for a secure payment gateway (https:// - URL with a padlock symbol).
3) Keep the PIN (Personal Identification Number), password, credit, or debit card number, CVV, etc., private and avoid disclosing the private financial information to friends or family members, banks, or other third parties.
4) Avoid keeping credit card information on websites, gadgets, shared laptops, and desktops.

[34] https://bnwjournal.com/2020/07/17/pune-citibank-mphasis-call-center-fraud/

[35] https://www.casemine.com/judgement/in/5dcfeb5146571b7a2b3af6b8

[36] https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf

5) Where two-factor authentication is an option, enable it.
6) Never respond to or open emails from unfamiliar sources as they may include phishing links or suspicious attachments.
7) Never give copies of your chequebook or your KYC documents to total strangers.
8) Use a virtual keyboard whenever possible on public devices because compromised gadgets, keyboards, etc. can also record keystrokes.
9) Immediately after use, log out of the internet banking session.
10)Passwords should be updated on a regular basis.
11)Use different passwords for your internet banking and email.
12)Avoid conducting financial transactions on public computers (such as those found in cybercafés, etc.).
13)By visiting your local branch or phoning the official customer service number listed on the bank's website, you can block not just the debit card or credit card but also the debit in the bank account connected to the card. Once the debit/credit cards, etc., are stopped as a result of a fraud, examine and assure the safety of alternative financial channels, such as net banking, mobile banking, etc. to prevent the fraud from continuing.\
14) Report the event via the National Cybercrime Reporting Portal (www.cybercrime.gov.in), by calling the hotline number 155260 or 1930, or both.
15)Reset Mobile: If a fraud has taken place as a result of a mobile device's data leak, use (Setting-Reset-Factory Data) to reset the mobile device.
16)If you would not be using your credit or debit card for a time, you should deactivate a number of functions and only activate them when you need to use the card. These capabilities include online transactions for both domestic and foreign purchases.
17)Similarly, if the card is not going to be utilised, the Near Field Communication (NFC) capability needs to be turned off.
18)You must carefully examine the amount displayed on the POS machine screen and NFC reader before entering the PIN at any Point of Sale (POS) site or while using the card at an NFC reader.
19)Never allow the retailer to take your card out of your sight as you swipe it during a transaction.
20)At a POS terminal/ATM, enter the PIN while covering the keypad with your other hand.

RBI has also facilitated to make complaints in case of any frauds through:

1. RBI Ombudsman:

- For filing complaints online, please visit the link at https://cms.rbi.org.in/
- Complaints by email can be sent to crpc@rbi.org.in.
- Complaints in physical / paper form can be sent to CRPC, Reserve Bank of India, Central Vista, Sector -17, Chandigarh -160 017.

2. Cyber Crime Police Station:

- National Cybercrime Reporting Portal - https://cybercrime.gov.in
- Cyber-crime reporting toll free number - 1930

8. Conclusion

With the emerging trend of cyber-crimes and increasing rate of frauds due to the increasing dependency on the internet, it is necessary for the Government and the Reserve Bank of India to work along with each other and construct stricter laws and stringent guidelines for the consumers. It must also be made point by the Government and RBI to increase the cyber literacy as dependency on technology has become inevitable. It must also be noted that the ambiguity about the governing law over cyber crimes makes conviction of the perpetrators unorderly, hence necessary amendments are also required to be made to the Information Technology Amendment (Act), 2008 is to be to condense the penalties to the actual crime based on the emerging trends. Since the IPC, 1860 laws are overridden by the IT Act, 2000, which governs cybercrimes, there are numerous situations where the IPC provisions are applied based on the unique circumstances of each case. The IT Act of 2000 does not adequately address many cybercrimes, notwithstanding the opinion of some that the IPC should not have a jurisdiction over them. Therefore, the IPC can be removed from governing in areas of cybercrimes after the necessary amendments are made to the IT Act, which contains provisions with regard to every cybercrime. Through the various literatures, it was also identified that Cohen and Felson (1979) Routine Activity Theory has significant impact on cyber-crimes as the theory contends that by viewing their interaction as "delayed" in time, motivated offenders and suitable targets can be brought together while being separated in time. Routine Activity Theory is not applicable in all parts of cyber-crimes; however, it is very much applicable in cases regarding cyber financial frauds.[37] Hence, it could be concluded that with the growth of technology and the increased reliance on internet and technology, the crimes on cyber space, especially loss of financial wealth is more significant and consequential to the victim than conventional crimes and necessary steps must be taken by the Government to increase the area of jurisdiction, within the country and develop cross border relationship to increase the rate of conviction and accountability.

[37] Eric Rutger Leukfeldt & Majid Yar (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis, Deviant Behavior, 37:3, 263-280, DOI: 10.1080/01639625.2015.1012409