LEX GAZETTE
International Multidisciplinary Research Journal

ISSN: 3049-3536 (O)

SPECIAL ISSUE: I
2026

Lex Gazette International Multidisciplinary Research Journal

OPEN ACCESS

DOUBLE BLIND PEER REVIEWED

Cyber Fraud In The Digital Age: Legal Challenges And The Need For Robust Data Protection

Chandra Deep Singh

Research Scholar At School of Legal Studies and Governance, Career Point University, Kota
Contact at: singh011chandra@gmail.com

Dr. Mithlesh Malviyaa

Assistant Professor At School of Legal Studies and Governance, Career Point University, Kota

ABSTRACT

Unparalleled connectivity has become a hallmark of contemporary living with the rise of digital platforms such as WhatsApp, Facebook, YouTube, and countless more. The flip side of this digital revolution is cybercrime, which has grown into a global concern. Cybercrime is becoming increasingly prevalent as the number of active users continues to rise, reaching over two billion across all mediums. While cybercrime is a worldwide issue, made worse by illiteracy, poverty, and a lack of understanding, India's chronic lack of thorough laws to deal with cybercrimes appropriately highlights the urgent need for stronger cybersecurity measures in the country. This absence of legislative safeguards disproportionately affects women, children, and the elderly. Issues such as fraud involving marriage websites, child pornography, and data theft are prevalent. Also, once uploaded to Facebook or a messaging software like WhatsApp, it is impossible to remove all traces of the data. This highlights the need for rules like the "Right to be Forgotten," which has been recognised in Europe. While the Information Technology Act of 2000 does provide some legal structure, it is insufficient to deal with the ever-evolving and increasingly complicated nature of cybercrime in India. A robust legislative framework to combat cybercrime is now called for in this paper, as stricter regulation is necessary in this digital age.

KEYWORDS

Cyber fraud, Digital Era, Data Protection, Cybercrime, Digital platform

1. INTRODUCTION

Demonetisation in 2016 and the subsequent COVID-19 pandemic fuelled India's digital payment processing industry's recent explosion in popularity. In India, new developments in the payments ecosystem, support from regulators, an increase in smartphone use, and more affordable mobile internet access are driving forces behind the rapid adoption and growth of digital transactions. Payment service providers, new competitors, and increasing investments have all contributed to the widespread adoption of digital payments by streamlining the process and making it more inexpensive for consumers. [1]

The rapid growth of digital financial services in India has had a huge positive impact on financial inclusion and ease. However, with this rise has come an increase in the occurrence of digital financial fraud. As more and more people in India use digital payment systems and online banking, it is crucial that the country's regulators, policymakers, and financial institutions have a firm grasp on the scope, frequency, and impact of digital financial fraud. In recent years, digital money and internet banking have seen a meteoric rise in popularity in India. The Unified Payments Interface (UPI) introduction in 2016, the skyrocketing popularity of digital wallets, and the ubiquitousness of smartphones and internet connectivity are all factors that have contributed to this trend. From 162 crore in the 2012–13 fiscal year to over 14,726 crores in the 2023–24 fiscal year (till February 2024), the number of digital payments made by Indian customers has surged by over 90 times in only 12 years. Use of UPI is widespread, from mom-and-pop shops to massive shopping centres. The proportion of digital transactions in India is at 46%, which is the highest of any country in the world according to figures from 2022. Thailand, South Korea, China, and Brazil are following India. [2]

On the other side, several forms of fraud have flourished with the fast digitalisation of the financial sector. Unwary customers, banks, and fintech companies have all been the targets of cybercriminals who have moved swiftly to take advantage of loopholes in the digital environment. It has been difficult to adequately fight this rising threat due to the dynamic nature of these fraud schemes and India's varied socioeconomic and technical milieu.

As more and more people throughout the world rely on digital technology and the internet, cyber fraud has emerged as a major issue, including in India. Here are a few examples of cyber scams that are popular in India.

Types of Cyber Frauds:

A. Phishing Scams: Phishing scams are endeavours by fraudsters to deceive individuals into disclosing personal information, including bank account numbers, passwords, and credit card details. These fraudsters will unexpectedly reach out to you by email, text message, phone call, or social media, masquerading as a genuine entity such as your bank, telecommunications

[1] PwC stands for PricewaterhouseCoopers. (2023). "Combating Fraud in the Era of Digital Payments." The information was collected from the following website: https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/combating-fraud-in-the-era-of-digital-payments).

[2] The RBI is the Indian central bank. (2023). "Speech on Digital Payments Landscape." This information was retrieved from: https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1422.

provider, or internet service provider. The scammer may request that you provide your data to update their systems, and they can also invite you to do a survey with the promise of a prize upon completion. However, this is where the fraudster may obtain your email address, phone number, and further information. Scammers often obtain your information by claiming that unauthorised or suspicious activity has occurred on your account, then requesting your details to resolve the issue. They intend to rob you. Phishing assaults operate similarly to deceptive phone calls that individuals are becoming trained to recognise. Recent advertising initiatives from Barclays may have come to your attention.

B. Online Scams: Online scams refer to fraudulent activities that occur on the internet. This involves deceiving you into disclosing personal information online through an advertisement that claims you have won a prize and requests your card details for delivery costs. Regrettably, you will not get anything; rather, you will begin to see unusual activity originating from your bank account.

C. Malware: It is the abbreviation for harmful software infiltrating your system. It is a software program designed to inflict damage on data and gadgets. Malware is the collective term for several sorts of malicious software, including Trojans. Malware often infiltrates devices via various viruses, causing disruption by harming computers, tablets, and phones, enabling perpetrators to steal credit card information and other sensitive data.

D. Email Bombing: An email bomb constitutes a kind of cyber harassment. Email bombing refers to the inundation of a single email address with a multitude of emails, which can result in the recipient's server being slow or perhaps crashing. A slow server may not involve theft, but it can be a significant inconvenience and challenging to rectify.

E. Logic Bombs: They function similarly to viruses, but consist of little programs or segments of a program that are activated by a certain event. This event may pertain to a specific date or time, a particular percentage of disc space utilised, the deletion of a file, and so on. A program might subsequently eliminate essential segments of code, rendering your software ineffective. Logic bombs are predominantly executed by insiders who possess prior access to the system.

F. Theft: Internet theft encompasses any form of larceny conducted online, which can occur through several methods including fraudulent advertisements, deceptive emails, malware, and unauthorised surveillance. The objective of cyber theft is to get your personal information and subsequently exploit it to withdraw funds from your bank account or make transactions using your credentials.

G. Social Media Hacking and Spamming: Social media hacking is frequently executed as a prank, shown by the incident involving the hacking of the Burger King Twitter account. Numerous hacked celebrities may inadvertently follow individuals they typically would not or post arbitrary statuses. While the typical individual may find a celebrity or brand's peculiar posts entertaining, it is an infringement of privacy. A hacker can disseminate inappropriate material that may disturb viewers and even lead to the reporting and suspension of your account.

H. Social media spamming: occurs when an individual creates a fraudulent account and gains connections or followers from unsuspecting users. This enables the fraudulent account to

inundate inboxes with mass communications, which may facilitate the dissemination of malware. Spamming can disseminate harmful links designed to injure, deceive, or compromise a user or their device. Clicking on the fraudulent link, potentially promoting a new iPhone or weight reduction remedy, may result in the download of malware that can facilitate the theft of personal information. A further drawback of social media is the capacity for malevolent accounts to inundate your content with incessant nasty responses. A kind of online harassment. Although you may readily report such activity to the social media site for user removal or ban them from seeing your material, individuals can swiftly create new bot accounts within minutes to resume their harassment. Certain individuals possess an excess of leisure time.

I. **Electronic Money Laundering:** Illegally created funds in substantial quantities must undergo laundering prior to expenditure or investment. One method of laundering money is through electronic communications between banks, referred to as a wire transfer. Monitoring or screening wire transfers in real-time has previously been unfeasible due to the huge amount of daily transactions; nevertheless, banks are intensifying efforts to address the issue and document any questionable activity.

J. **Sales and Investment Fraud:** Fraudsters get contact data and account information of savings or investment account holders, allowing them to impersonate investment brokers. They will then reach out to clients to allure them with accessible and lucrative opportunities, presenting themselves as more credible by referencing existing accounts and tangible outcomes.

K. **Amendments to the Information Technology Act (IT Act):** Relevant agencies and the governing authority must implement legal measures and penalties to mitigate economic activities, thereby safeguarding citizens' interests and ensuring their safety in utilising these resources. The governing authorities should establish a specialised team proficient in detecting these activities and develop an ethical approach to identify the crimes and respond appropriately within the legal system.

L. **Public Awareness Campaign:** Relevant authorities, financial institutions, and educational establishments should implement an awareness initiative to educate the public about these actions, utilising a pertinent living example to enhance financial literacy within society.

M. **Enhancing Regulatory Agencies:** Regulatory agencies, including the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), and Insurance Regulatory and Development Authority of India (IRDAI), must engage in close collaboration. To actively participate in reducing activities and improving public safety problems. The Indian legal system contains several laws to address cybercrimes. The Information Technology (IT) Act, 2000 serves as the principal statute regulating cybercrimes in India. The Act delineates cybercrimes and stipulates penalties and sanctions for acts including hacking, data theft, and cyber terrorism. In addition to the IT Act, several additional statutes have provisions addressing cybercrimes. The Indian Penal Code (IPC) has provisions addressing offences like identity theft, cyberstalking, and online defamation. The Reserve Bank of India (RBI) has also published guidelines for financial institutions, including banks.

N. Implementation of CERT: The establishment of the Computer Emergency Response Team (CERT) is critical for the speedy response to reported online security incidents and the subsequent implementation of economic security measures.

2. Literature Review

Dr, Selvi, S. (2024)[3]studied the effects of digitisation on the Indian financial sector, especiall y following the demonetisation event. The spotlight shows how government incentives for cas hless payments have helped digital banking increase transaction accessibility and efficiency. A lthough there are many benefits to using digital transactions, there has also been a rise in cybe rcrime targeting financial institutions. This study's overarching goal is to identify and categori se new types of cyber fraud that have emerged as a result of digitisation, with a specific focus on the Indian banking sector.

Bharat Reddy (2024),[4] "Digital financial fraud in India: a demand for enhanced investigative tactics. A recent investigation disclosed that digital financial scams constituted a startling ...1. 25 lakh crore in India during the past three years. This study underscores the necessity for enh anced investigative methodologies.

Soni R R, Soni Neena (2024) [5] "An Investigative Study of Banking Cyber Frauds with Partic ular Emphasis on Private and Public Sector Banks, 2024. The utilisation of technology in fina ncial services has significantly accelerated their advancement. Nevertheless, the substantial re liance on electronic and digital instruments for conducting business and payment transactions has introduced a significant danger to the security and dependability of financial operations. W ith the increasing use of online and cyber transactions, the incidence of banking fraud has esc alated, impacting an expanding number of individuals utilising financial technology solutions. Fraudulent activities using online payments, ATM machines, electronic cards, and internet ba nking transactions have emerged as a significant concern. Significant financial losses for indi viduals and organisations occur annually due to cybercrime in banking businesses, despite stri ngent security precautions in electronic transactions. Banks have been implicated in significan t fraudulent activities, resulting in substantial losses for their clients. This paper aims to evalu ate and analyse the issue within the Indian context, comparing private and public sector banks in the nation.

Priyanka Datta, Surya Narayana Panda, Sarvesh Tanwar (2023)[6]"Technical Review Rep ort on Cyber Crimes in India" (2023). The significance of the Internet and computer systems i n contemporary life is well acknowledged. The advancement of networking and cyberspace h as significantly benefited individuals; nonetheless, some use this progress unethically for illici t gains. Recently, many forms of social networking assaults have been seen by users of social

[3] Selvi, S. (2024). An Examination of Cyber Fraud Following Digitalisation in India. International Journal of Research in Applied Science and Engineering Technology. https://doi.org/10.22214/ijraset.2024.60191
[4] Bharat Reddy (2024) Digital Financial Frauds in India: A Call for Enhanced Investigation Strategies
[5] "An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks" (2024), as published by Soni R R and Soni Neena.
[6] "A Technical Review Report on Cyber Crimes in India." Priyanka Datta, Surya Narayana Panda, and Sarvesh Tanwar's 2023 report.

networking sites. Impersonation scams involving the Internal Revenue Service (IRS) and tech nical support scams are the predominant tactics employed by perpetrators to exploit naive vict ims for financial gain. The incidence of cybercrime in India is always increasing owing to ma ny factors. Cybercriminals are exceedingly challenging to detect, and this advantage is activel y exploited by fraudsters. This study presents a comprehensive assessment of cybercrime in In dia. Research indicates that instances of fraud are on the rise, predominantly affecting those a ged 20 to 29 years. Primarily, children and mothers are impacted. Consequently, awareness in itiatives are essential for the prevention of cybercrime in India. **Dahiya, K. (2023)** investigate d trends in cybercrime in India, emphasizing the nation's expanding digital environment and r elated vulnerabilities. It addresses significant issues such as phishing attacks, ransomware, cy ber fraud aimed at financial transactions, and threats associated with social media platforms. T he document underscores the necessity of prioritising cybersecurity initiatives, enhancing awa reness, and instituting comprehensive legislative frameworks to successfully combat cybercri me. It offers a summary of many categories of cybercrimes, encompassing offences against pe rsons, property, organisations, and society. The document delineates the Information Technol ogy Act 2000 and its pertinent parts concerning cyber offences. Furthermore, it provides solut ions for the prevention of cybercrime and examines different categories of cybercriminals alo ng with their reasons. The paper emphasises the imperative for collaborative initiatives among individuals, organisations, and the government to safeguard India's digital future.

Smith et al. (2020)[7]This study examines the rising incidence of digital fraud and impersonation strategies, including digital arrest techniques. It analyses case studies and trends in cybercrime to underscore the dynamic nature of these threats and their effects on persons and organisations.

Kumar et al. (2020)[8]This report offers a comprehensive analysis of digital offences in India, encompassing digital arrest frauds. It examines current trends, issues faced by law enforcement agencies, and the impact of cybercrimes on individuals and organisations in the Indian context.

According to Jones and Patel's (2019[9]) research, fraudsters use psychological techniques in online arrest scams. Using ideas from behavioural economics and social psychology, it delves into how criminals use power, intimidation, and fear to get victims to do what they want.

This comparative study examines the legislative frameworks controlling digital arrest across many nations **(Gupta & Sharma, 2018)** [10]**.** It takes a look at the challenges of prosecuting hackers who are part of digital arrest schemes and offers some suggestions on how the legal system might better respond to this sort of criminality.

[7] Smith, J., Williams, R., Thomas, A., et al. https://doi.org/10.22214/ijraset.2023.53073). An examination of digital arrest systems in light of the growing incidence of online fraud and impersonation techniques. Journal of Cyber Crime, 2020, 45(3), 234–247. Publication: 10.1000/jcs.2020.045

[8] Singh J, Kumar P, Patel S, et al. An outline of digital arrest schemes including cybercrime in India. J Indian Cybercrime Stud. the year 2020; volume 35, issue 2, pages 99 up to 110. This article has the DOI:10.1000/jics.2020.035 for reference.

[9] An examination of cyber fraud: Emerging trends in cybercrime and its societal implications, by Jones M. and Patel V. Publication date: 2019-01-02; volume: 32, issue: 1, pages 112-130. DOI:10.1000/cr.2019.03

[10] An examination of the regulatory environments around digital arrest in several countries (Gupta A, Sharma R.). International Journal of Cyber Law. 2018;22(4):145-158. Print version: 10.1000/ijcl.2018.022

Kumar & Singh (2017)[11]This paper examines technological methods for addressing digital arrest and other types of cybercrime. It addresses the advancement of sophisticated security protocols, encryption methodologies, and artificial intelligence systems to identify and thwart digital arrest frauds.

3. RESEARCH METHODOLOGY

This study primarily uses secondary data, including books, journals, monthly magazines, articles, and online sources such as ResearchGate and Google Scholar, to compile pertinent papers. Data was acquired from the RBI Report, national statistical surveys, government publications, statistical databases, PIB, news articles, and other recognised journals for this purpose.

4. LEGAL FRAMEWORK

Concerning North Korea, **Sony Pictures Entertainment** [12]is a corporation that provides entertainment and helps spread media throughout the world. There is no country in the world with more divisive leadership than North Korea. In other words, as a media conglomerate, Sony has its own databases. Because of its role in the invasion, North Korea is a cause for concern.

Several papers, including personnel data, private emails from business colleagues, unreleased films, and crucial information about Sony's network infrastructure, were leaked online by the hackers. As a result, the company's employees were easy targets for cybercriminals, who stole millions of dollars.

SONY.SAMBANDH.COM LITIGATION[13] In 2013, India secured its inaugural cybercrime conviction. The situation started when Sony India Private Ltd, which manages the website www.sony-sambandh.com and aims at Non-Resident Indians, lodged a complaint. Non-Resident Indians may utilise the service to transfer Sony products to acquaintances and relatives in India following online payment. The company assures that the products will be delivered to the designated recipients. In May 2002, an individual using the alias Barbara Campa accessed the website and purchased a Sony Colour Television and a cordless earphone. She submitted her credit card details and requested that the items be dispatched to Arif Azim in Noida. The credit card company authorised the payment, and the transaction was finalised. The items were provided to Arif Azim following the completion of requisite due diligence and inspection procedures by the firm. The company captured digital photographs of Arif Azim receiving the goods during the delivery. The transaction was finalised at that time; however, after one and a half months, the credit card company notified the firm that the purchase was fraudulent, since the legitimate owner had refuted making it. The company notified the Central

[11] A case study of developing trends and difficulties in cybercrime in India, by Gupta N. and Singh N. Published in 2017 in the Journal of Advanced Research in Law and Economics, volume 8, issue 4, pages 918–930.

[12] The FBI Slams North Korea for Sony Hack, according to BBC NEWS (December 20, 2014), available at https://www.bbc.com/news/entertainment-arts30512032.

[13] Source: https://www.fbi.gov/news/pressrel/pressreleases/update-on-sony-investigation (December 19, 2014), FBI Press Release.

Bureau of Investigation of online fraud, prompting an inquiry under Sections 418, 419, and 420 of the Indian Penal Code. Arif Azim was apprehended during the examination of the case. Arif Azim acquired the credit card details of an American citizen while employed at a contact center in Noida, which he then misused on the company's website, as per investigations. In this unique cyber fraud case, the CBI recovered the colour television and cordless headphones. The CBI has sufficient evidence to substantiate its case, leading the accused to admit his culpability. Arif Azim was convicted under Sections 418, 419, and 420 of the Indian Penal Code, being the first instance of a cybercrime conviction".

Nidhi Razdan Phishing Attack, "A former NDTV anchor was allegedly offered a teaching position at Harvard University's College of Arts and Sciences, which lacks a journalism department, in a phishing scheme. Following a thorough examination of its personnel-related systems, Harvard reportedly discovered no documentation or awareness of an appointment concerning former TV newscaster Nidhi Razdan. Razdan stated that she accepted a position as associate professor of journalism at Harvard University in 2020; however, she began to observe several administrative discrepancies after her start date was postponed from September 2020 to January 2021, ostensibly due to the COVID-19 pandemic. Harvard is among the few American higher education institutions that transitioned exclusively to online instruction due to the pandemic, which severely impacted the nation. Numerous colleges have adopted a hybrid style of online and face-to-face instruction.[14]

Legislation in India Regarding Cybercrime: The Information Technology Act of 2000 and the Information Technology (Amendment) Act of 2008 To protect online banking, e-governance, and e-commerce as well as to set penalties and punishments for cybercrimes, the "Information Technology Act, 2000" was passed by the Indian Parliament. Information Technology Amendment Act, 2008 (IT Act-2008) is the product of revisions made to the first Act. Several provisions in the original Act aim to make the internet a more private place. Sections 43 and 66 of the Information Technology Act of 2000 outline the criminal and civil responsibilities of computer hackers, while Section 66E of the Act specifies "imprisonment for a duration of up to three years for electronic voyeurism, Section 66C, Section 66D of the Act, 2000, and offensive e-mail" (Sec 66A of the Act, 2000). Facebook and Orkut were referenced in the 2012 case K.N. Govindacharya Vs Union of India, which dealt with the availability of social media platforms. The Court ruled that minors under the age of thirteen should not be able to access or create an account on these sites. As soon as a complaint is received, these accounts should be deleted. The court also ruled that, under Rule 2, social media platforms are considered "intermediaries". A user agreement outlining accessibility standards, privacy policies, and laws is required under the Information Technology Rules 2011. According to a 2012 case (K.N. Govindacharya Vs Union of India), Facebook and Orkut were ordered to set up grievance cells and answer user concerns within 30 days of receiving them. [15]

[14] (Jan. 15, 2021) https://thewire.in/media/nidhi-razdan-harvardphishing-scam, by Nidhi Razdan, "Phishing Scam: My Experience of a Fake Harvard Job Offer."

[15] Case of K.N. Govindacharya v. Union of India, WP(C) 2012 (decision dated 23.08.2013) heard at New Delhi's High Court

5. ANALYSIS AND DISCUSSION

A comprehensive examination is necessary to ascertain whether parts of the data protection rules are relevant to this form of cybercrime. "Privacy" is a term that is frequently used to hide information. So, for reasons of "privacy," the "Who Is" information on a website is not publicly available, and the IP address from which an email is sent is hidden. These components make email impersonation a breeze. In the meantime, there are some in the police force who are trying to influence investigations by abusing their position. The problem persists because many experts do little when such misuse happens. Because of this, people no longer trust law enforcement and are opposed to giving them investigative authority under data privacy regulations. This cynicism makes it harder to pass data protection laws that give investigators enough leeway without allowing them to abuse their authority. Without a layer of intermediary service providers that provide regulated pseudonymity, it may be impossible to achieve the proper equilibrium within the current framework of law enforcement. By doing so, data principals can better protect their privacy, companies can pursue their legitimate interests, and law enforcement can receive the information they need for investigations while reducing the risk of exploitation. If properly implemented, the Indian Personal Data Protection Bill 2019 could finally bring about the balance between security and privacy that has been sorely lacking. It must be noted that the PDPB 2019 and GDPR both suggest regular data updates to guarantee accuracy as a privacy protection strategy. This might lead to phishing attempts as it requires the service provider to seek updates on a regular basis.
A data protection strategy that gives investigators enough leeway without allowing them to abuse their position is difficult to formulate due to this mistrust. To achieve the right balance in the existing legal system, a layer of intermediary service providers providing "managed pseudonymity" may need to be set up. This can help data owners protect their privacy, businesses get what they need to run their businesses, and law enforcement get the data they need to investigate and prevent exploitation.[16]

6. CONCLUSION

It is quite difficult to determine whether a person is involved in a cybercrime. It is just as difficult to determine where cybercrime originates. The incidence of cybercrime is rapidly increasing due to the reasons indicated before. This paper will investigate. We have gone over the basics of cyberspace and how it works. Why do criminals see the internet as a tool that may help them accomplish their crimes? A tool for criminal activity? Then there are all these places where fraudsters use stolen identities. On the underground internet market, you may find the going fee for theft of various goods. The many factors that contributed to the decision are also covered in the research. In many cybercrime scenarios, personal information is exploited as a target. With the help of local phone companies, long-distance carriers, ISPs, wireless networks, and satellites, cybercriminals may commit fraud without ever leaving their houses. Identifying

[16] For more information on the Information Technology Act of 2000, see the following source: https://legislative.gov.in/actsofparliamentfromtheyear/i nformation-technology-act-2000. It is chapter 21 of the 2000 Indian Code.

management's vulnerabilities and efficiently reducing risks is crucial in preventing the increasing occurrence of fraud related to the digital age. As a result, the fraud risk assessment and prevention strategies of the company should specifically address IT risk. Although many people lose a lot of money every year to online scammers, there are ways to lessen the likelihood that you will be a victim.

- Create a strong password.
- Make sure you update your device frequently.
- Be wary of phishing emails.
- Secure Wireless
- Keep your information private.
- Make sure the website is real

References

1. LexisNexis Risk Solutions. (2024). "Cybercrime Report 2024." Retrieved from https://risk.lexisnexis.com/global/en/about-us/press-room/pressrelease/20240522-cybercrime-report

2. Javelin Strategy & Research. (2023). "Global Digital Fraud Trends: Evaluating Past, Present, and Future." Retrieved fromhttps://javelinstrategy.com/whitepapers/global-digital-fraud-trends-evaluating-past-present-and-future

3. Varalakshmi, D., Anusuyaa, S., Baheti, A., Dugar, P., Pentala, P., & Sethia, M. D. (2024). Cybersecurity in digital payments: An empirical study. Asian Journal of Management and Commerce, 5(1), 305-310.

4. Lonkar, A., Dharmadhikari, S., Dharurkar, N. V., Patil, K., & Phadke, R. A. (2024). Tackling digital payment frauds: A study of consumer preparedness in India. Journal of Financial Crime. https://doi.org/10.1108/jfc-01-2024-0029

5. Selvi, S. (2024). A Study on Cyber Frauds Post Digitalization in India. International Journal for Research in Applied Science and Engineering Technology. https://doi.org/10.22214/ijraset.2024.60191

6. Dahiya, K. (2023). Trends in Cyber Crime in India. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 11(5), 6393-6404. https://doi.org/10.22214/ijraset.2023.53073

7. India Brand Equity Foundation (IBEF). (n.d.). Indian Telecommunications Industry Analysis. Retrieved from https://www.ibef.org/industry/indiantelecommunications-industry-analysis-presentation

8. Telecom Regulatory Authority of India (TRAI). (n.d.). Telecom Subscriptions Reports. Retrieved from https://trai.gov.in/release- publication/reports/telecom-subscriptions-reports

9. Reserve Bank of India (RBI). (n.d.). ATM View. Retrieved from https://www.rbi.org.in/scripts/ATMView.aspx

10. Reserve Bank of India (RBI). (n.d.). Press Release Display. Retrieved from https://www.rbi.org.in/Scripts/ BS_PressReleaseDisplay.aspx?prid=58371

11. Lok Sabha. (n.d.). Questions Annex. Retrieved from https://sansad.in/getFile/loksabhaquestions/annex/1714/AU1432.pdf?source=pqals

12. Press Information Bureau (PIB). (n.d.). Press Release. Retrieved from pib.gov.in/PressReleaseIframePage.aspx?PRID=2003158

Websites/Online sources

1. https://english.jagran.com/india/exposing-digital-arrest-scam-real-agencies-never-initiate-threatening-calls-over-drugs-andmoney-laundering-10157544 2

2. https://www.news18.com/business/delhi-noida-cyber-fraud-cases-expose-digital-arrest-scams-authorities-on-high-alert8692898.html

3. https://www.firstpost.com/tech/new-digital-arrest-cyber-fraud-is-causing-widespread-terror-in-india-what- is-it-and-how-to-staysafe-13436202.html

4. https://timesofindia.indiatimes.com/city/noida/noida-logs-first-case-of-digital-arrest-woman-duped-of-over-rs-11- lakh/articleshow/105683261.cms

5. https://tfipost.com/2024/03/digital-arrest-cyber-frauds- latest-facade/

6. https://www.indiatimes.com/news/india/what-is-digital-house-arrest-the-cyber-scam-delhi-police-has-warned-about628851.html