# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 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

# ONLINE BANKING FRAUD

AUTHORED BY - RUGVED JAGTAP
'C-40' BBA.LLB Third Year (2023-2024)
Bharati Vidyapeeth Deemed to be University New Law College, Pune

## *Abstract*

***This research paper examines the rise of online banking frauds in the twenty-first century, which is beingdriven by technical innovation and a growing move towards digital banking. It discusses a variety of scams,including vishing, phishing, fraudulent applications, skimming, Wi-Fi vulnerabilities, wire transfer fraud, and social media impersonation, as well as preventive measures including caller ID verification and encryption techniques. It investigates the causes of the increase in scams, including the advent of online marketplaces, the popularity of peer-to-peer payments, advances in banking, and technical sophistication.Case studies such as the Punjab National Bank Fraud and the Bank of Baroda Black Money Scam demonstrate the scope and complexity of such frauds, emphasizing the importance of strong cybersecurity measures and legislative changes to protect the banking system and global economies in the digital era.***

## INTRODUCTION:

Within the 21st century, our everyday lives are overwhelmed by innovation. We need everything to be doneimmediately, our quick approach towards each angle of our life made changes in the way we approach everything in our daily lives. As able to see, there's tremendous growth in each segment, counting managing account administrations, we want online managing an account instead traditional keeping money framework,which requires our physical nearness for each benefit. Online keeping money can be done wherever we are,and the exchange can be done within a few minutes, and it's accessible 24 hours a day. As the development within the managing an account segment makes a difference to us with swift service, it moreover carries thechance of online managing account extortion. It makes shoppers lose money. Within several seconds, most are ignorant of the conceivable chance of online managing an account. Online banking still has not reached its flawlessness; in this way, we must be mindful of the conceivable hazard of using modern innovation for our consolation. Web managing an account is broadly utilised to check

ISSN: 2582-6433

subtle elements, make buys, pay bills,transfer stores, print articulations, etc. For the most part, the client character is the client character number, and asecret word is given to secure exchanges. But due to a few obliviousness or senseless botches, you'll effectively fall into the trap of cybercriminals.

## Scams in Online Banking

### 1. *Vishing*

Frauds acting as investors, firm officials, protection operators, government authorities, and others call or approach clients over the phone or social media. Fakers unveil several buyer actualities, such as the customer's title or date of birth, to win belief. Frauds may weigh or trap clients into sharing private data such as passwords, OTPs, PINs, and Card Confirmation Values (CVVs) by citing an urgency or crisis suchas the got to square an unauthorized exchange, an instalment required to dodge a punishment, or an

appealing markdown, among other things. Clients are at that point duped by utilising these accreditations.[1]

### 2. *Phishing*

Phishing is the movement that extraordinary to 'fish' your private money data. It may include getting amail that supposedly appears to be from a well-known institution like a bank or a trusted site. You must be mindful of this and not press on such emails. Note that your bank would never ask for your private data, such as your watchword, login subtle elements, or OTP, among other such data.

### 3. *Frauds due to the utilize of obscure or unconfirmed portable apps*

Agreeing with the RBI, fraudsters circulate through SMS, mail, social media, Moment Courier, etc. certain app joins, and conceal to seem comparative to the existing apps of authorized substances. Fraudsters trap the client into pressing on such links, which come about within the downloading of obscure or unconfirmed apps on the customer's versatile, portable workstation, desktop, etc.

[1] Sneha Kulkarni '10 types of banking frauds in India customers should know about' (The Economic Times, 25 March 2022)
<https://economictimes.indiatimes.com/wealth/save/10-types-of-banking-frauds-in-india-customers-should-know-about/articleshow/9 0438911.cms?from=mdr> (last accessed 28 January 2024)

ISSN: 2582-6433

Once the noxious application is downloaded, the fraudster picks up the total get to the customer's gadget. These incorporate secret points of interest put away on the gadget and messages or OTPs gotten sometime recently or after the establishment of such apps.[2]

### 4. ***Skimming***

To commit this extortion, scammers usually hide a little contraption called a skimmer within the cardspaces of ATMs or shipper installment terminals, which can examine and record your card data. Fraudsters indeed utilizea carefully set camera to record your Stick. It is prudent to remain caution at whatever point you visit an ATM booth to anticipate such managing an account extortion.[3]

### 5. ***Open Wi-Fi systems***

Open organizing is continuously troublesome, as open Wi-Fi gives programmers adaptability to get toindividual data. As it were, if the client employs the web in eateries, office stores, and air terminals, dothey unwillingly grant their device access to the go-getter?

It can be exceptionally simple to hack the gadgets of the clients in the event that they are utilizing private data on an open organization that does not require a password.

On the off chance that you open your bank account online by utilizing open WiFi, at that point unconsciously, your points of interest will be uncovered, making your account defenceless to bank fraud. Too, in the event that you're doing web-based shopping with the assistance of open Wi-Fi, at that point you may uncover your credit card data, which is inclined to chance.

### 6. ***Wire Exchange Extortion***

The term “wire transfer” originated from the practice of exchanging stores between banks over transmit wires.Wire Exchange Extortion ordinarily happens in one of two

[2] ibid
[3] “Understanding Skimming and How to Prevent It” <https://www.flagright.com/post/understanding-skimming-and-how-to- prevent-it> (Accessed on: 26 January 2024)

ISSN: 2582-6433

ways:

A scammer poses as a true person, merchant, company, or family member and demands a wire exchange, regularly deceiving the casualty sincerely by claiming it's a crisis. For example, an employee in a fund gets anemail from the CEO asking for cash to be exchanged with a merchant by the near end of commerce, or the bargain will drop through. The email includes the account dataand looks genuine, but it isn't.[4]

A programmer may screen mail communications around a wire exchange and alter the wireenlightening todivert the reserves to a distinctive account.

With individuals getting more comfortable sending cash online, wire exchange extortion is expanding, as is thevalue of each exchange. One Ponder shows that the average value is up about 68% from Q2 2020, coming to $12.5K in Q4 2021.

### *7. Impersonation on social media*

With parcels of individuals investing time on social media and upgrading their subtle elements, fraudsters have made it simple to induce subtle elements to trick the individuals. As per the RBI booklet, "Fraudsters make fakeaccounts utilizing points of interest of the clients of social media stages such as Facebook, Instagram, Twitter, etc. Fraudsters at that point send an email to the users'companions inquiring for cash for pressing therapeutic purposes, installments, etc. Fraudsters, utilizing fake subtle elements, contact clients and pick up users' beliefs over a period of time. Whenthe users' share their individual or private data, the fraudsters utilize such data to shakedown or blackmail cash from the users."

## Measures for prevention[5]

### *1. Vishing*

Verify Caller Identities: Encourage people to confirm the identities of callers before disclosing any critical information. They should inquire about the caller's name,

[4] "Wire Fraud Laws: Overview, Definition and Examples" (Investopedia, November 3, 2023) <https://www.investopedia.com/terms/w/wirefraud.asp> (Accessed on 30 January 2024)

[5] Peterson, K. (no date) 5 tips to prevent online fraud, Banner Bank. Available at: <https://www.bannerbank.com/financial- resources/blog/tips-to-prevent-online-fraud> (Accessed: 30 January 2024).

ISSN: 2582-6433

organization, and a call-back number.If the caller claims to be from a real organization, the individual should independently check the contactinformation and call back using the official number shown on the organization's website or other reliable sources.

Implement Caller ID Authentication: Use technologies like Secure Telephony Identity (STI) or Caller ID Authentication to check the legality of incoming phone calls. These technologies can assist identify fake caller IDs and lower the likelihood of vishing attacks.[6]

Voice Biometrics: Wherever possible, use voice biometrics solutions. Voice recognition technology canvalidate callers' identities based on their distinct voice patterns, offering an extra degree of security to phone communications.

Establish Call handling processes: Create explicit processes for managing phone calls, particularly thoseasking for sensitive information or presenting as urgent. Employees should understand how to escalateunusual phone calls and report possible phishing efforts to the proper authorities within the organization.

### 2. ***Phishing***

Use Email Filtering and Spam Detection: Use email filtering and spam detection software to automatically identify and quarantine questionable emails. These solutions can help limit the amount of phishing emails thatreach users' inboxes while also providing an extra layer of security against phishing attempts.

Enable Multi-Factor Authentication (MFA): Set up multi-factor authentication (MFA) for important systems andaccounts. MFA increases security by forcing users to give two forms of verification, such asa password and a one-time code texted to their mobile device, lowering the chance of unauthorized accesseven if credentials are stolen via phishing attacks.[7]

Implement Web Filtering and URL Scanning: Use web filtering and URL scanning

[6] Sarit, "What Is a Vishing Attack | Examples & Prevention | Imperva" <https://www.imperva.com/learn/application-security/vishing-attack/> (Accessed on: 27 January 2024)
[7] Simister A, "How to Recognize Phishing Attacks and 10 Ways to Avoid Them" (Lepide Blog: A Guide to IT Security, Compliance and IT Operations, January 31, 2024) <https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/amp/> (Accessed on: 27 January 2024)

ISSN: 2582-6433

technologies to prevent access to known harmful websites and detect phishing sites in real-time. These solutions can assist prevent usersfrom mistakenly accessing phishing sites and falling victim to credential theft or malware infestations.

Monitor and Analyze Email Traffic: Look for signals of phishing activity, such as increases in suspiciousemail volumes or patterns of phishing-related phrases. Analyse email records and user reports to detect possible phishing attempts and take preventative actions to reduce risk.

### *3. Frauds due to the utilize of obscure or unconfirmed portable apps*

App Reputation Services: Use app reputation services and security solutions to learn about the reputation and trustworthiness of mobile apps. These services look at app behavior, permissions, and other characteristics todetect potentially malicious or counterfeit apps.

App authenticity Verification: Use techniques like digital signatures or app attestation services to ensure the legitimacy of mobile apps. These techniques serve to guarantee that the apps have not beentampered with oraltered by third parties.

### *4. Skimming*

Use EMV Chip Technology: Encourage the adoption of EMV (Europay, Mastercard, and Visa) chip- enabled cards, which provide more security than standard magnetic strip cards. EMV chip technology creates dynamic transaction codes that are difficult for fraudsters to reproduce, making it more difficult toskim card information.

Install anti-skimming devices: Install anti-skimming devices or security overlays on payment terminalsand ATMs to prevent unauthorised access to card readers and guard against skimming attempts. Thesedevices candetect and stop skimming attempts by preventing access to the card's magnetic stripe or chip.

Secure PIN Entry: Use PIN shields or privacy screens to prevent unauthorised parties from viewing or recordingPINs during transactions. Encourage consumers to conceal the keypad when inputting PINs toreduce the risk oftheft.

ISSN: 2582-6433

### 5. ***Open Wi-Fi systems***

Use Encryption: To secure Wi-Fi networks, use encryption technologies such as WPA2 (Wi-Fi ProtectedAccess 2) or WPA3. Encryption scrambles data sent across a network, rendering it illegible to unauthorised individuals attempting to intercept it.

Use Strong Passwords: Set strong and unique passwords for Wi-Fi networks to prevent illegal access. Avoid using the default passwords given by router manufacturers since they are frequently easy to guessor well-known.

Enable Guest Networks: If feasible, set up guest networks with limited access rights for guests or temporary users. Guest networks should be kept separate from the main network and have limited accessto important resources.

### 6. ***Wire Exchange Extortion***

Implement Email Authentication: Use email authentication protocols like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) to verify email sender authenticity and detect spoofing or fraudulent emails.

Use secure communication channels: Encourage the use of secure communication methods, such as encrypted email or messaging platforms, when sending sensitive data or discussing financial transactions.Avoid transferring critical information via unencrypted or unsecured channels.

### 7. ***Impersonation on social media***

Verified Accounts: Encourage users to verify their social media accounts, particularly corporations, prominent people, and organisations. Verified accounts are characterised by a blue checkmark, allowingusers to differentiate genuine profiles from imposters.[8]

Report Impersonation: Encourage users to report suspected impersonation or fake

[8] Us_Jporta, "Social Media Impersonation: What Is It? How to Stop It" (Red Points, December 21, 2023) <https://www.redpoints.com/blog/social-media-impersonation-what-is-it-how-to-stop-it/> (Accessed on 29 January 2024)

ISSN: 2582-6433

accounts to the appropriate social media networks. Most platforms offer built-in reporting systems for impersonation, trademark infringement, and other policy breaches. Prompt reporting can help to remove impostor accounts more quickly.

Implement Two-Factor Authentication: To add degree of protection to your social media accounts, use two-factor authentication (2FA) or multi-factor authentication (MFA). When signing in to an account with 2FA, users must give extra verification, such as a temporary code texted to their mobile device.

## Reasons behind the Increase in scam

1. The appearance of modern commercial centre stages:

   From social systems and dating apps to nourishment conveyance, elective transportation, and get- away rentals, advanced channels have revolutionized nearly every industry. All through this year, country-wide quarantines have caused an indeed more noteworthy spike in portable application utilization, with buyers requesting the conveyance of everything from foodstuffs to automobiles. Withthe increasing number of commercial centre stages and administrations accessible and their broad notoriety, particularly in the later months, fraudsters have moved their strategies to take advantage ofrising in-app and online commercial centre purchases.

2. Installments are moving online:

   In addition to customers executing more in online marketplaces, they are also utilizing peer-to-peer(P2P) and eWallet apps more regularly. These apps are most prevalent in Europe and Asia but are becoming progressively prevalent within the U.S. as well, with 71% of Americans saying they haveutilized a P2P instalment stage. Clients turn to these stages to carefully part supper checks with companions, send cash to family individuals in other parts of the world, pay for administrations from a nearby merchant, and more. But with more than half of P2P exchanges taking place between shoppers and an obscure substance, the extortion hazard is high.

3. Progressively advanced keeping money administrations:

   Today's shoppers request more online and versatile services from their money-related education. Asaresult, bequest banks are going advanced. They are doing more account onboarding and exchange endorsements online and deemphasizing in-person

ISSN: 2582-6433

exchanges, which makes it harder to confirm characters. Moreover, in reaction to shopper requests, an unused breed of “challenger banks"—bornanddoing commerce totally within the online world—have risen and are separating themselves by providingeasy-to-use and digital-native encounters. A lion's share of these institutions' clients is thosewho have “thin file” credit histories (i.e., do not have much credit information). Less information implies a more noteworthy hazard of extortion.

4. Technological Advancements:

Nowadays, extortion has, moreover, quickened and developed more modernly due to the rise of e- commerce, versatile instalments, and computing control. Numerous of the same innovations that companies depend on to improve and quickly present modern items and services are also being received by fraudsters.[9] Offenders can more effortlessly commit extortion by utilizing cheap, on- demand compute control or convey calculations utilizing machine learning that is more unpretentious and competent at controlling extortion discovery frameworks. The conventional rules-based extortionavoidance frameworks that organizations have depended on for a long time presently battle to keep up.

## Cases related to online banking scams

- Punjab National Bank (PNB) Fraud - Nirav Modi and Mehul Choksi[10]

The Punjab National Bank (PNB) fraud, spearheaded by jewellers Nirav Modi and Mehul Choksi, shook India's financial landscape in 2018, revealing unauthorized transactions surpassing $2 billion.Exploiting vulnerabilitiesin PNB's procedures, they leveraged fraudulent Letters of Undertaking (LoUs) to secure loans before absconding from the country. The scandal laid bare systemic deficiencies in risk management and oversight within India's banking sector, sparking regulatory overhauls and legal actions to bring the culprits to justice. Thecase spotlighted the imperative for robust internal controls and heightened vigilance to prevent such large-scale financial misconduct. Furthermore, efforts to extradite Modi and Choksi emphasized the necessity for global collaboration in tackling cross-border financial crimes. Ultimately, the PNB fraud underscored the importance of transparency,

[9] “Inside the Rise of Bank Fraud in India - IDFY” (IDfy, January 23, 2024) <https://www.idfy.com/blog/inside-the-rise-of-bank- fraud-in-india/> (Accessed on 29 January 2024)
[10] 'Major Bank Frauds in India: A Deep Dive into the Deceptions and Loopholes' (test book, 28 August 2023) <https://testbook.com/static-gk/major-bank-frauds-in-india> (last accessed 29 January 2024)

ISSN: 2582-6433

accountability, and regulatory integrity to safeguard the integrity of financial systems and restore public trust in banking institutions.

- Vijay Mallya Scam[11]

  The Vijay Mallya scandal is around the failure of Kingfisher Airlines and charges of financial irregularities involving the Indian businessman. Kingfisher Airlines, founded in 2005, aspired to provide a premium flying experience but quickly suffered operational and financial issues. By 2012,the airline had discontinued operations, leaving significant obligations to creditors, including banks and workers. Investigations indicated that monies intended for the airline were reportedly syphoned away for personal use and redirected to other Mallya-owned businesses. Mallya's opulent lifestyle, which included costly parties and the purchasing of sports teams, garnered attention during the airline's financial troubles.

  Subsequent investigations by Indian authorities revealed cases of financial mismanagement and illegal behaviour inside the Kingfisher Group. Mallya fled India for the United Kingdom in 2016 due to rising pressure from legal and investigative agencies. The Indian authorities launchedextradition proceedings to return him to face allegations of fraud and money laundering. Despite lengthy legal fights and appeals, extradition processes persisted in British courts. The case highlightsconcerns about corporate governance, financial responsibility, and the difficulties of prosecuting high-profile persons accused of financial malfeasance in many jurisdictions.

  According to the most recent developments, Mallya's extradition is delayed, prolonging the legal battle over his suspected role in the Kingfisher Airlines case.

# Conclusion

In conclusion, the expansion of online banking, although providing unsurpassed ease, has exposed peopleand institutions to an increasing number of sophisticated frauds. From vishing and phishing to fraudulent mobile applications and wire transfer fraud, cyber threats are constantly exploiting technical breakthroughs. Mitigatingthese threats necessitates a

[11] Ruchi Gupta 'Electronic Banking Frauds: The Case of India' (ResearchGate, September 2023) <https://www.researchgate.net/publication/291297679_A_Proposed_Framework_to_Prevent_Financial_Fraud_through_ATM_Card_Cloning.> (last accessed 29 January 2024)

ISSN: 2582-6433

multidimensional strategy that includes public awareness, education, and broad use of advanced security features like biometric authentication and encryption. Notable incidents, such as the Punjab National Bank scam and the Vijay Mallya scandal, show the need for regulatory change and increased enforcement. As we traverse the digital era, we mustwork together to strengthen the security of online banking,therefore preserving trust and confidence in the financial institutions that are critical to our connected world.