INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL ARREST SCAMS IN INDIA; ASSESSING THE ADEQUENCY OF LEGAL FRAMEWORK AND ITS IMPACT ON DIGITAL ECONOMY AND FINANCIAL STABILITY

AUTHORED BY - V.ANESHA
Sastra Deemed University

ABSTRACT:

Digital Arrest scams have been on the rise in India as a form of cyber enabled fraud in india In These Scams Offenders may act as Police Officers, Investigating Agencies, customs officials or other authorities and threaten victims with arrest or legal action So That They pay them Money The Scam uses Technological Deception with Psychological Manipulation and often involves using digital communication channels and electronic payment system

This Paper Studies Digital Arrest Scams From Perspective of Legality, Institutional and economic Aspects. The relevant Provisions Of The Information Technology Act 2000 And The Bharathiya Nyaya Sanhita 2023 Are analysed the role of the Indian Cyber Coordination Centre 14((C), The National Cyber Crime Reporting Portal (NCRP) The 1930 Helpline and The Citizen Financial Cyber Fraud Reporting And Management System (CFCFRMS) Are Discussed the paper also Analyses the connection between digital arrest scams, digital payments, the Digital economy and broader cyber-related Financial risks

This Paper Adopts a Doctrinal methodology and analyses legislation, judicial decision, government Documents, Peer Reviewed Literature and Institutional Reports The Paper shows that Indian Law Already has many Provisions that can be used to deal with the conduct that constitu Digital arrest scams However There are Still Problems with Fund Freezing, Fund restoration, cross-border investigation, identification, identification of mule accounts and coordination among different institutions. The Paper therefore proposes strengthening preventive mechanism increasing financial intervention, improving institutional coordination and Raising Public Awareness

ISSN: 2582-6433

Key Words Digital Arrest Scams, Cyber Fraud, Information Technology Act 2000, Bharatiya Nyaya Sanhita 2023, 14C, Digital Payment System, Financial Stability Digital Economy, Mule Accounts, Fund Recovery

1.1 INTRODUCTION:

The use of Digital technology has become a normal part of everyday life in India. people depend on smartphones, internet service, online banking, UPI and other digital payment facilities for both personnel and commercial transactions. [1]This helps to develop quicker and more convenient in financial transaction However The same digital environment has also created new opportunities for cyber criminals. One of the more form of cyber enabled financial fraud is the so called digital arrest scam In a typical digital arrest scam, the offender pretends to be police officer, customs and official investigating officer or some other government authority. The Victim is informed that their name, mobile number, bank account, identity document or parcel has been connected with the criminal offence. This caller then creates a sense of fear by claiming that the victim is often instructed to transfer the money on the pretext of verification, security, bail or some other fabricated legal requirement.

The scam is particularly serious because it does not depend only on technical banking, instead the offender uses psychological pressure and the victim's respect for government authorities to obtain money. The victim may receive video call, fake notice, photograph of officials, fabricated documents or other material intended to make the communication appear genuine. It is important to clarify that Digital Arrest is not legally recognised form of arrest under Indian Law A person cannot be legally placed under arrest simply by being kept on a video call or by being threatened over the telephone the expression is mainly used to describe a method adopted by cybercriminals to make victims believe that they are facing official criminal proceedings. The supreme court of India Has also recognised the seriousness of such crime and has dealt with the digital arrest as a distinct form of cybercrime.

This research therefore examine digital arrest scams from three connected prospective legal and institutional and economic it looks at the provision of the information technology act 2000and the bharatiya nyaya sanhita 2023 and also consider the role of institutions such as the

[1] 11 Years of Digital India: Better Healthcare & Digital Markets Making Lives Easier. http://www. pib. gov. in/PressReleaseDetail. aspx?PRID=2280068&reg=1&lang=1. Accessed 1 Oct. 2026.

ISSN: 2582-6433

Indian Cyber Coordination Centre, 14(C), National Cyber Crime Reporting Portal (NCRP), 1930 Helpline and CFCFRMS The Study Also consider the effect of these scams on digital payments and the wider digital economy While an Individual Cyber Fraud Does not automatically create Financial Instability repeated cyber fraud can create cost for victims, banks, payment service providers and government agencies it may also influence public confidence in digital financial service

1.2 EVOLUTION OF CYBERCRIME AND EMERGENCE OF DIGITAL ARREST SCAM

Cybercrime has changed considerably with the development of the internet and digital technologies, in its earlier stages computer relegated crime was often associated with activities such as unauthorised access to computer systems, data, theft, malware and interference with computer networks.[2] As internet use became more widespread, criminals began using technology for identity theft, phishing, online impersonation and other forms of deception. The Growth Of Online has added another dimension to cybercrime. Criminals no Longer need to Physically access a victim's bank or personnel belongings. Through a Phone Call, message or online platform they can manipulate a person into transferring money themselves

Digital Arrest scams are an example of this changing nature of cybercrime. they combine Traditional forms of cheating and impersonation with modern communication technologies Offenders may use video calls, fake government documents, manipulated images, Uniform and simulated offices to create an appearance of official authority The Increasing use of digital communication during and after the COVID 19 period also contributed to a social environment in which many official and financial activities could be conducted remotely. This convenience, However also created opportunities for criminals to imitate legitimate interactions

The Important feature digital arrest is therefore not simply the technology used by the offenders. The scams succeeds because technology is combined with social engineering. the offender creates a believable situation, establish apparent authority and then uses fear and urgency to prevent the Victim From Checking Whether The Communication is Genuine

1.3 MEANING AND NATURE OF DIGITAL ARREST SCAM:

A Digital Arrest Scam is a Fraudulent Scheme in which a person is falsely informed that they are involved in a criminal investigation and that immediate action is necessary to avoid arrest

[2] Wolf, Arctic. 'History of Cybercrime'. *Arctic Wolf*, 19 Apr. 2024, https://arcticwolf. com/resources/blog/decade-of-cybercrime/.

ISSN: 2582-6433

or other legal consequences. [3]The Scam generally begins with an unexpected communication. The Offender may claim that a parcel containing illegal goods has been booked in the victim's name or that the victim's Aadhar details, SIM card or bank account have been connected with an alleged offence

The Victim may Then be transferred to another person who is introduced as a senior police officer, investigating officer or other government official this makes the conversation appear more credible in some cases the offenders remain connected with the victim through a video call for long periods and instruct the victim not to speak to anyone else the psychological element is central to the scam. A Person who believes that they are speaking to a genuine police officer may be less likely to question the allegations. The threat of immediate arrest creates further pressure and reduces the time available to independently verify the information

Recent Research has also examined susceptibility to digital arrest scams by focusing on factors such as fear, authority and compliance. this indicate that the scam is different from ordinary phishing because the offender does not simply ask the victim to click on a fraudulent link instead, thus, digital arrest scams can be understood as a combination of impersonation, social engineering, psychological manipulation and financial fraud

1.4 MODUS OPERANDI OF DIGITAL ARREST SCAMS:

Although the exact method may differ from one case to another, digital arrest scams generally follow a similar pattern. First the offender contacts the victim through a telephone call, messaging platform or another digital communication service. The offender introduces themselves as a police officer, customs official, investigating officer or representative of another authority.

The Victim is then informed about an alleged criminal activity. For Eg the Offender may claim that a parcel, bank account, mobile number or identity document belonging to the victim has been connected with an illegal transaction after creating fear the offender may introduce another person as a senior officer. Fake uniforms, identity cards, Police station backgrounds government logos and fabricated legal documents may be used to make the interaction appear genuine

In some cases, the victim is told to stay constantly on the video call. They may be instructed not to end the call, talk to family members, or reach out to the police on their own. This stops the victim from getting help from others and lets the offenders keep control over their mental

[3] What Is Digital Arrest Fraud and How Can You Avoid It?' *Vaishali Bhagwat*, https://vaishalibhagwat. com/how-to-avoid-digital-arrest-fraud. Accessed 1 Oct. 2026.

ISSN: 2582-6433

state. The last step typically includes asking for money. The offender might call the payment a security deposit, verification fee, bail money, or a temporary transfer needed for an investigation. After the victim sends the first payment, the offender may ask for more money by coming up with another fake legal reason.

The funds might be moved through multiple accounts. Mule accounts are often used to receive and transfer the money, which makes it more difficult to trace the actual person in control of the funds[4]. In some situations, the money may also be transferred between different states or countries. This method demonstrates that digital arrest scams should not be considered as straightforward communication fraud. These scams involve several steps, starting with impersonation and culminating in the movement of money through the financial system.

1.5 STATEMENT OF RESEARCH PROBLEM:

In India, digital arrest scams have become a significant type of cyber-enabled financial fraud. Even while current laws address identity theft, intimidation, extortion, personation, cheating, and computer-related offenses, it can be challenging to actually police these laws when criminals use cutting-edge technology and operate across borders

A significant issue stems from the rapid pace at which illicit funds can be moved. Before a victim realizes they've been tricked, the funds might have already moved through several accounts. Mule accounts, counterfeit identities, and international networks can complicate the processes of tracing and recovery. This issue also has a broader scope since these scams utilize the identical digital payment systems employed by countless genuine users

The primary research question is if India's current legal and institutional structure is adequately prepared to thwart digital arrest scams, probe offenders, seize and recover illegally transferred funds, and safeguard the broader digital payment system and digital economy.

1.6 RESEARCH OBJECTIVES:

1. To examine the Nature, Characteristics and methods used in digital arrest scams in India.
2. To Analyse the relevant Provision of the Information Technology act 2000 and the Bharatiya Nyaya Sanhita in relation to digital arrest scam
3. To Examine the role of 14c, NCRP, the 1930 helpline and CFCFRMS in responding to cyber financial fraud

[4] What Is a Mule Account? Detection Signals, Investigation Steps, and Reporting. https://sphinxhq. com/blog-posts/what-is-a-mule-account-detection-investigation. Accessed 1 Oct. 2026.

ISSN: 2582-6433

4. To Examine the effect of Digital arrest scams on institutional difficulties involved in preventing and investigating such scams
5. To suggest measures that may improve prevention, financial intervention, investigation and recovery of fraudulent funds

1.7 RESEARCH QUESTION:

1. To what extent does the existing Indian legal framework adequately address the conduct involved in digital arrest scams?
2. What legal and practical gaps affect the investigation and prosecution of digital arrest financial intervention?
3. What institutional and procedural difficulties affect the tracing, freezing and recovery of fraudulently transferred funds?
4. How may digital arrest scams affect confidence in digital payment system and the wider digital economy
5. What legal, technological and institutional measures and could strengthen India's response to digital arrest scams

1.8 SCOPE AND LIMITATION:

This research is mainly focused on digital arrest scams in the context of the Indian legal and financial system. The legal part of the paper involves the analysis of the Information Technology Act 2000, Bharatiya Nyaya Sanhita 2023, and other related procedural and evidentiary legislation. The institutional aspect of the study includes such I4C, NCRP, 1930 helpline, CFCFRMS, and other mechanisms involved in detecting suspicious accounts and preventing the withdrawal of funds. The economic analysis is mainly devoted to the impact of digital arrest scams on victims, financial institutions, digital payment systems, and the digital economy in general. International sources are mainly used to highlight the general relationship between cyber risks and financial stability.

Among the main limitations of the present study, the first one is the recently emerged nature of the threat, which makes it difficult to obtain statistical data that would fully quantify the economic impact. Moreover, government reports may actually combine digital arrest scams with other types of cyber fraud, making the comprehensive assessment difficult. Another limitation is that the paper concentrates on doctrinal issues related to the topic. In other words, it uses legislative acts, court decisions, government reports, academic research, and other documents for analysis. However, there are no empirical sources, including interviews or field

ISSN: 2582-6433

surveys, since the research is descriptive rather than applied. Finally, note that cybercrimes in general and digital arrest scams in particular are less likely to be reported or recorded, which does not allow getting precise statistics. Nonetheless, the legal and institutional basis seems to be sufficient for the current level of analysis and identification of potential issues.

CHAPTER 2

2.1 LITERATURE REVIEW:

Digital Arrest Scams are a comparatively recent area of cybercrime research as a result, the academic literature specifically dealing with this form of fraud is still developing, however the available studies provide useful information about the psychological, legal, technological and financial aspects of the problem S James Robert, Varsha Singh, Ravi p Pandey and Bismirty Bhuyan have examined digital arrest from a psychological perspective. Their work explains that these scams are based heavily on fear, authority and pressure to comply the Offender creates a situation in which the victim believes that a genuine government authority is speaking to them the Fear of Arrest or legal action then makes the victim more likely to follow the instructions given by the fraudster[5]

Another study by S James Robert focuses specifically on susceptibility to digital arrest scams. The research attempts to measure the factors that make individuals vulnerable to this type of fraud. The Study is useful because it shows that digital arrest cannot be understood only as a technical cybercrime. The behaviour of the Victim and the psychological pressure created by the offender are also important part of scam

Legal research has also examined the wider legal and ethical issue surrounding digital arrest scams, Nisha and Jitender Singh Dhull discuss they way offenders misuse their name and the identities of law enforcement agencies another authorities. their question also raise question about whether existing legal mechanisms are sufficiently responsive to new forms of technology based deception[6]

The role of banks and telecommunication service providers has been discussed by Eshan Singhal and Nitin Tripathi. Their research highlights the importance of cooperation between financial institutions, telecom companies and law enforcement agencies. This is particularly relevant because a digital arrest scam often involves both communication technology and

[5] Pubmed. Ncbi. Nlm. Nih. Gov. https://pubmed. ncbi. nlm. nih. gov/41858474/. Accessed 1 Oct. 2026.
[6] Journal, IJLLR. 'Digital Arrest Scams In India: Evaluating Legal Responses And Public Awareness'. *IJLLR Journal*, 15 Aug. 2026,
https://www. ijllr. com/post/digital-arrest-scams-in-india-evaluating-legal-responses-and-public-awareness

ISSN: 2582-6433

financial institutions.

Harsh gaur has examined the legal and investigative difficulties involved in digital arrest fraud. The research points towards such as mule accounts,, digital evidence, technological tools and the difficulties faced by investigating agencies when the people involved in the scam operate through different jurisdiction

The existing literature therefore provides useful information about individual aspect of digital arrest scams however there is still scope for examining the issue from a combined legal and economic perspective. Much of the available research focuses on psychological vulnerability criminal law or investigation comparatively ess attention has been governed to how digital arrest scams interact with digital payment system and the wider digital economy

This research attempts to address that gap by bringing together legal provision, institutional response and economic consideration it does not treat digital arrest scam only as a problem of individual cheating instead it examine how the increasing use of digital financial service has created both opportunities and challenges in dealing in dealing with this from of cyber fraud

2.2 RESEARCH METHODOLOGY:

The Present Study follows a doctrinal method of legal research. the Min sources used for the study include legislation, judicial decision and government publications, institutional reports academic articles and other relevant secondary materials, The information technology act 2000 and the bharatiya nyaya sanhitha 2023 form an important part of the legal analysis. the study examine how provision relating to cheating, personation, identity related offences, intermediation and computer related offences may apply to conduct associated with digital arrest scams

Judicial orders are also examined because the court have had to respond to the practical difficulties created by these scams in particular the continuing proceedings before the supreme court concerning victims of digital arrest have provided information about issue such as mule accounts, financial intervention, investigation, restoration of money and coordination between different institutions, Government materials are used to understand the functioning of 14C, NCRPP the 1930 helpline CFCFRMS and the suspect registry. These sources are especially useful for examining the practical mechanism available for reporting cyber fraud and attempting to stop fraudulent funds from being moved further

The research also consider international material on cyber risk and financial stability such material is used only for understanding the broader economy and not for assuming that digital arrest scams have independently caused systematic financial instability in India the information

ISSN: 2582-6433

collected from these sources in analysis to identify the legal provision applicable to digital arrest scam the strengths and limitI on of existing institutional mechanism and the possible effects of such fraud on the digital economy. Since the study is preliminary doctrinal it does not use primary survey data or or statistical hypothesis testing. the hypothesis is instead used as an analytical proposition against while the existing legal and institutional framework is examined

2.3 LEGAL FRAMEWORK GOVERNING DIGITAL ARREST SCAMS IN INDIA:

There is currently no Separate Offence under Indian Law Called Digital Arrest The Expression is used To describe a method of fraud rather than a legally recognised type of arrest depending upon the facts of a Particular case, different provision of criminal and cyber law may apply

2.3.1 INFORMATION TECHNOLOGY ACT 2000

The Information Technology act 2000 remains one of the Principal laws dealing with offences involving computers, electronic communication and digital information

Section 43 deals with certain unauthorised acts involving computer system and providers for compensation, where the acts covered by sec 43 are committed dishonestly or fraudulently, sec 66 may may become applicable and gives the conduct criminal consequences[7]

Section 66C deals with identity theft it become relevant where an offender dishonestly uses another person's Electronic signature, password or other unique identification feature this can have significance in cases where personal credentials are misused during a cyber fraud

Section 66D is particularly important in digital arrest cases it deals with cheating by personation through the use of a communication device or computer resource since digital arrest scams commonly involve telephone calls, online communication and video call in which the offender pretends to be a government official, this provision may apply where its ingredients are established

Section 72 and 72A may also become relevant in appropriate cases involving disclosure or misuse of information. section 75 deals with certain offences involving conduct outside India where the statutory conditions concerning computer resources or system located in india are satisfied. section 78 deals with investigation of offences under the information technology act

The IT Act therefore provides several tools that can be used against technology assisted fraud however not every aspect of a digital arrest scam necessarily falls within the IT act. The

[7] Information Technology Act 2000,

ISSN: 2582-6433

underlying conduct may also involve offences under the general criminal law

2.3.2 BHARATIYA NYAYA SANHITA, 2023

The Bharatiya nyaya sanhita 2023 is important because many digital arrest scams involve traditional criminal conduct carried out through technology

Section 318 deals with cheating, where a victim is dishonestly deceived and is thereby induced to deliver property or act in manner causing wrongful loss the provision may become relevant sec 319 specifically deals with cheating by personation[8]

These provisions are particularly relevant because the core of a digital arrest scam is often the false representation that the offender is a police officer, CBI officer, customs, official, judicial authority or another government representative

Depending on the facts, provision concerning extortion or criminal intermediation and forgery may also apply for eg where threats are used to obtain money the relevant provisions concerning extortion or criminal intermediation may be considered similarly if forged warrants, notice, identity cards or court documents are used, provisions relating to forgery and use of forged documents may become relevant

The important point is that digital arrest scams do not necessarily require a completely new criminal offence to be prosecuted. Existing offences can address many parts of the conduct the practical difficulty lies in identifying the offender, collecting electronic evidence, tracing the money and connecting the different individuals involved in the fraud

2.3.3 BHARATIYA SAKSYA ADHINIYAM 2023

Electronic evidence is central to digital arrest investigation, call recordings, whatsapp message, emails, screenshots, bank transaction records, video calls, ip related information and digital documents may all become relevant

The Bharatiya sakhya adhiniyam 2023 provides the legal framework concerning evidence, including electronic record, investigators therefore need to ensure that digital evidence is properly collected, preserved and presented before court [9]

This become particularly important in cases involving fabricated documents or manipulated video and audio material a fake government order or digitally altered document may look genuine to the victim but can become important evidence once its source and authenticity are investigated

[8] Bharatiya Nyaya Sanhita 2023
[9] Bharatiya Nyaya Sanhita 2023

ISSN: 2582-6433

2.3.4 NEED FOR A COMBINED LEGAL APPROACH

Digital arrest scams show how cyber crime law and criminal law now overlap simply using phone or video call does not automatically make an act an offence under IT act the actual conduct still has to be checked For this reason, prosecuting a digital arrest scam usually needs more than one law working together the IT act BNS and the Procedural law and evidence law no single law is enough by itself

The harder question is not whether the act is punishable in most cases, it is already. The harder question is practical: how fast can the police find the offender, stop the money from moving further and get it back to the victim?

2.4 INSTITUTIONAL FRAMEWORK FOR PREVENTION AND RESPONSE

Law alone cannot stop digital arrest scams because digital money moves within seconds fast acting institutions matter just as much as the law itself

2.4.1 INDIAN CYBER CRIME COORDINATION CENTRE(14C)

14C was set up by Ministry of home affairs to improve coordination in handling cybercrime it works with police, other agencies on prevention, public awareness, investigation, training it began as a scheme in 2018 and become a formal attached office of the ministry of home affairs from 1st july 2024[10]

14C main value is coordination. cybercrime usually crosses state and institutional lines and information held by one agency is often needed by another. A central body helps connect police, banks, telecom operators

2.4.2 THE NATIONAL CYBER CRIME REPORTING PORTAL(NCRP)

NCRP is the online portal where the public reports cybercrime it is part of the 14C system and is meant to make reporting easy Reporting fast matters, because early reporting increases the chance of stopping or tracing the money but reporting alone does not guarantee recovery the bank still has to verify the transaction, place a hold, trace where the money went next, and follow legal procedure before anything is restored[11]

[10] INDIAN CYBER CRIME COORDINATION CENTRE (I4C).
https://www. pib. gov. in/www. pib. gov. in/Pressreleaseshare. aspx?PRID=2223095. Accessed 1 Oct. 2026

[11] Ministry of Home Affairs, Government of India, 'About I4C' (Indian Cyber Crime Coordination Centre) <https://i4c. mha. gov. in> accessed 1 October 2026.

ISSN: 2582-6433

2.4.3 1930HELPLINE

The 1930 helpline lets victims report financial cyber fraud immediately, its purpose is to cut down the time between the fraud and the report since digital money can move between accounts in minutes a delay of even a few hours can make recovery much harder A victim who reports right away has a far better chance of stopping the money than one who waits several days[12]

2.4.4 CITIZEN FINANCIAL CYBER FRAUD REPORTING AND MANAGEMENT SYSTEM(CFCFRMS)

CFCFRMS was launched in 2021 under 14c enable immediate reporting of financial fraud and stop funds from being further moved as of 30 June 2026 more than 11, 158 crore had been saved through this system across more than 32. 80lakh complaints from about 8600 crore across 24. 65 lakh complaints as of 31 January 2026 showing how quickly the system use has grown over just few month by june 2026 1, 586 entities, including 40 foreign banks operating in india, had been onboarded onto the platform from April 2026, the system also added the money restoration module and a grievance redressal module which help victim to recover their fund and raise complaints. The amount reported as saved does not mean that the amount is has already been returned to the victims, it usually means that the money was stopped frozen or kept and hold the money restoration module introduced 2026 helps in returning such money but the actual recovery depends on investigating and legal procedure

2.5 JUDICIAL RESPONSE

Origin of the Supreme court

The Supreme Court Of India Took suo motu cognisance of digital arrest scams on 17th October 2025 after receiving a complaint from a 73 year old woman and her husband from ambala, haryana. the couple stated that they had been contacted by a person pretending to be a officer of the CBI, intelligence Bureau and judiciary. They were threatened with arrest and other legal action were shown fake official documents as a result they transferred approximately 1. 05 crore through several bank transaction.

The Supreme Court Registered the matter as In Re:Victims Of Digital Arrest Related to Forged Documents, suo motu writ petition criminal no 3 of 2025 the court observed that the use of forged supreme court documents and the names of judges could affect public trust in judicial institutions the court issue notice to the concerned authorities including the ministry of home

[12] Kushwaha, Vikram Singh. 'You Called 1930 After a Cyber Fraud — What Happens Next?' Vikram Singh Kushwaha, May 2026, https://vikramkushwaha. in/blog/1930-cyber-helpline-bank-freeze-process/.

ISSN: 2582-6433

affairs, CBI, State of Haryana and the cyber crime department Ambala this proceeding is important because the supreme court intervention began with an individual complaint but later developed in individuL Complaint but later [13]developed into broader examination of digital arrest scams and their investigation across India

2.5.1 SUPREME COURT'DIRECTIONS ON INVESTIGATION:

On 1 December 2025 the supreme court issued further directions concerning the investigation of digital arrest scams. The court considered the interstate and cross border nature of these offences and directed that the CBI should undertake investigation on a pan India in appropriate cases

The court also directed technology intermediaries to corporate with investigating authorities and provide relevant information required for investigation if Further considered the issue of bank account suspected to contain money obtained through digital arrest scam and directed that appropriate steps to be taken where the funds were prima facia connected with a reported cybercrime

The court also needed differences in the approach of different high court regarding the freezing of bank account suspected of receiving fraud proceeds this show the practical difficulty of balancing effective investigation with the rights of genuine account holders[14]

2.5.2 HIGH COURT APPROACH TO FROZEN BANK ACCOUNT:

The High court also dealt with issue relating to the freezing of bank connected with cyber fraud in some cases courts have examined the role of mule accounts and the responsibility of account holer and banks these judicial developments shows that the digital arrest scams create two important legal concerns the first is the need for effective investigation and prevention of fraudulent transaction. the Second is need to protect genuine victims and innocent account holders from unnecessary restrictions therefore judicial intervention has focused not only on punishing offenders but also on improving investigation, freezing suspicion funds and facilitating the restrictions of money to victim

[13] In Re: Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Criminal) No 3 of 2025 (Supreme Court of India, Order dated 17 October 2025) (Surya Kant and Joymalya Bagchi JJ).

[14] M, Rizmi Lia. 'Digital Arrest Scams: What Has the Supreme Court Directed to Protect Victims?' *The Hindu*, 11 Aug. 2026. India. www. thehindu. com, https://www. thehindu. com/news/national/digital-arrest-scams-what-has-the-supreme-court-directed-to-protect-victims/article71332 091. ece.

ISSN: 2582-6433

2.5.3 INVESTIGATION AND CBI ROLE:

The supreme court proceedings also led to directions concerning investigation by the CBI in subsequent proceeding the court continued to monitor the implementation of measure relating to digital arrest cases by August 2026 the court recorded that the CBI had registered ten digital arrest cases one investigation reportedly involved 238 victims, 67 first layer bank accounts and transactions of approximately 80 crore with searches conducted across 16 state the court also considered whether the existing threshold for CBI investigation should be lowered and whether cases involving the same organised network should be considered together where the total amount involved crosses the relevant threshold. These development show the difficulty of dealing with organised cybercrime through isolated state level investigation when the same network may operate across several jurisdictions.

2.5.5 FINDING OF THE STUDY:

The examination of the legal and institutional framework leads to several findings First, Digital arrest scams are not based on technology alone. the offender combines technology with psychological manipulation the impersonation of police officer, investigating agencies or other official creates an appearance of authority, while threats of arrest create fear and urgency

Seconds the existing indian legal framework already contains several provisions that may be used against the conduct involved the IT act address certain forms of computer related offences, identity theft and cheating by personation through communication devices. The BNS provides provisions relating to cheating and personation and may be applied apply to intimidation extortion and forgery depending on facts

2.5.6 Impact on the Digital Economy

The digital economy depends largely on the use of digital communication, online banking and electronic payment systems. When a person becomes a victim of cyber fraud, the immediate impact is usually the loss of money. However, such fraud can also create other costs. A victim may lose personal savings, borrow money to meet financial needs, or spend additional money and time trying to recover the lost amount. Banks and other financial institutions also have to spend more on fraud detection, cybersecurity, customer support and compliance measures. Government authorities are required to use resources for investigation, digital forensics and creating public awareness.

Cyber fraud may also affect the confidence of people in digital services. A person who has lost money through a digital payment platform may become more careful about using similar

ISSN: 2582-6433

services in the future. Family members and others who learn about such incidents may also become cautious. However there is insufficient evidence to conclude digital arrest scam alone have caused a measurable decline in india digital economy. The available evidence does not separately measure the economic effect of digital arrest scams from other forms of cybercrime. Digital arrest scams can therefore be viewed as one of the risks associated with the rapid growth of the digital economy. As the use of digital financial services continues to increase, effective measures to prevent cyber fraud are important for maintaining public trust in digital services.[15]

2.5.7 Impact on Digital Payment Systems

Digital arrest scams are closely connected with digital payment systems because the main purpose of the fraud is usually to make the victim transfer money to the fraudster.

The speed of digital payments creates an additional difficulty in dealing with such fraud. Fraudsters can take advantage of this speed and transfer the money through different accounts before the victim reports the incident. Therefore, early reporting is very important. When a fraudulent transaction is reported quickly, banks and investigating authorities have a better opportunity to trace the receiving account and stop the money from being transferred further. The CFCFRMS and the Suspect Registry are examples of mechanisms developed to respond to this problem. At the same time, measures to prevent fraud must also protect legitimate account holders.

Financial institutions therefore need proper procedures for examining suspicious accounts, handling complaints and removing restrictions when the transaction is found to be genuine. The objective should not be to block as many transactions as possible.

2.5.8 Financial Stability: Indian and Global Perspective

Financial stability should be distinguished from the financial loss suffered by an individual. A person who loses money through a digital arrest scam may face serious financial difficulties. However, an individual fraud case, or even a large number of individual cases, does not automatically mean that there is systemic financial instability. Financial stability refers to the ability of the financial system as a whole to continue functioning without major disruption. Cyber incidents can become a financial stability concern when they affect major financial institutions, important payment infrastructure, market confidence or interconnected financial

[15] International Monetary Fund, Global Financial Stability Report (IMF) (general discussion of cyber risk as part of the broader risk environment facing financial systems). The author should verify and insert the exact edition, year and chapter/page reference before final submission

ISSN: 2582-6433

systems.

International financial institutions have also recognised that cyber incidents can create financial and economic risks. Such risks may arise from disruption of services, financial losses and loss of confidence in financial systems. The International Monetary Fund has considered cyber risk as part of the wider risks faced by financial systems.

This perspective is relevant to India because digital arrest scams operate through interconnected banking and payment systems. They are therefore part of the wider cyber-risk environment. However, the evidence considered in this study does not establish that digital arrest scams alone have caused systemic financial instability in India.

The more important concern is the cumulative effect of different cyber threats. Digital arrest scams occur alongside phishing, ransomware, identity theft, investment fraud, malware and other forms of cybercrime. If these risks continue to increase, their combined effect may place greater pressure on financial institutions and regulatory authorities. Therefore, strengthening cyber resilience is important not because every cyber fraud creates a systemic crisis, but because a highly digital financial system must be capable of dealing with repeated and interconnected cyber threats.

CHAPTER 3

3. CONCLUSION:

Digital-arrest scams are a particular form of cyber-enabled financial frauds because they combine technology with the elements of psychological manipulation and false legal authority. The aim is not merely to get the victim to provide information but rather is to make the victim believe that he or she has to act immediately or face arrest, seizure of property or other legal actions.

The study concludes that India does not lack criminal provisions to address this new form of fraud. The Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 cover a number of crucial aspects of such frauds, which include identity theft, cheating by personation, cheating, forgery, and use of forged electronic records. Also, criminal conspiracy is dealt with in Bharatiya Nyaya Sanhita, 2023. The Bharatiya Sakshya Adhiniyam, 2023 provides mechanisms to collect electronic evidence in such cases. But having criminal provisions covering most of the aspects of digital-arrest scams is only the first step in coming up with an effective response. The essence of such scams demands quick response and cooperation from diverse agencies depending on the particulars of each individual case. Police authorities, I4C,

ISSN: 2582-6433

banks and payment intermediaries, telecom service providers and digital platforms are important stakeholders in drafting an effective response system.

The Supreme Court proceedings that have been taken up by the Court are significant in that the response to digital-arrest scams is no longer limited to criminal prosecution and recovery of the financial losses suffered by the victim. The Court has taken up the issue of mule accounts, SIM misuse, grievance redressal, restoration of financial losses and banking safeguards.

The study therefore concludes that the central issue is not simply whether digital-arrest scams are punishable. They are. The more important issue is whether the legal and institutional system can prevent the transaction, trace the financial trail, preserve evidence, identify the perpetrators and restore the victim's money quickly enough.

With regard to the digital economy, the principal concern is the effect of fraud on trust, consumer confidence and operational resilience. Existing evidence supports concern about these effects, but does not justify concluding that digital-arrest scams alone have caused systemic financial instability in India.

The research objectives are therefore met by identifying a framework that provides substantial substantive criminal-law coverage but requires continuing development in preventive safeguards, coordination, financial recovery and victim protection.

CHAPTER 4

4. RECOMMENDATIONS AND FUTURE DIRECTIONS

Recommendations

4.1 Strengthen Public Awareness

Greater public awareness is necessary to prevent people from becoming victims of digital arrest scams. People should be clearly informed that there is no legally recognised process called a “digital arrest”. Awareness programmes should explain the common tactics used by fraudsters, including fake police or government calls,

video-call threats, false legal documents and demands for money.

4.2 Improve Immediate Financial Response

The 1930 helpline and CFCFRMS should be further strengthened to ensure that complaints involving fraudulent transactions are acted upon without unnecessary delay. Quick communication between the victim, bank and investigating authority can increase the possibility of stopping the money before it is transferred through additional accounts.

ISSN: 2582-6433

4.3 Strengthen Coordination Between Institutions

Effective action against digital arrest scams requires cooperation between different institutions. Police authorities, I4C, banks, telecom service providers and online platforms should have effective channels for sharing relevant information. Timely sharing of information can assist in identifying suspicious accounts, following the movement of funds and detecting organised fraud networks.

4.4 Improve Monitoring of Mule Accounts

Banks and financial institutions should continue to improve their systems for identifying and monitoring mule accounts. At the same time, there should be a proper process for checking accounts that have been wrongly identified as suspicious. This is important to ensure that genuine customers do not face unnecessary restrictions on their accounts.

4.5 Strengthen Digital Investigation

Digital investigations and cybercrime units need to be further strengthened. In 2020, over 1500 cases were registered under the PIDA. However, only around 600 were filed under the IPC. This points to a lack of digital commitment and informal engagement of the law enforcement authorities to deal with such cases. The suggestion is based on a report by GAP, prepared in consultation with the Architrave group and multicopper, that was officially shared with the Ministry of Home Affairs (MHA). The report acknowledges that “the slow investigation of cases involving digital arrest scams has led to many victims having little confidence in the effectiveness of law enforcement agencies and digital investigation teams. ” The report recommends strengthening digital investigation and cybercrime units and enhances training and infrastructure by taking community feedback into account.