STEGWARE-INDUCED FINANCIAL FRAUD: A LEGAL ANALYSIS OF BANKING REGULATION AND LIABILITY

Sreeja M, Sastra Deemed to be University

Nikitha Natchiyar G, Sastra Deemed to be University

ABSTRACT

The rapid growth of digital banking has increased the risk of cyberattacks aimed at banks and their customers. One such threat is stegware, which hides malicious software inside ordinary looking files such as PDF documents, images, invoices and bank statements. Unlike conventional malware, stegware can slip past firewalls and antivirus software. This raises serious legal questions about whether the banking regulatory framework can deal with covert threats, and who should bear the loss when customers are harmed.

This paper examines whether the Indian legal framework, including the Banking Regulation Act 1949, the Information Technology Act 2000 and the cybersecurity directions of the Reserve Bank of India (RBI), adequately obliges banks to prevent and detect stegware-based attacks. It also analyses how liability should be divided among banks, customers and payment gateways when an unauthorised transaction results from hidden steganographic malware. The study follows a doctrinal method, analysing statutes, regulatory guidelines, judicial precedents and comparative practice. It argues that existing regulations set general cybersecurity obligations but neither address covert steganographic attacks nor lay down clear standards of liability for them, and it proposes reforms.

Keywords: Stegware; Steganography; Banking Cybersecurity; Unauthorised Electronic Transactions; Customer Liability; RBI Framework.

I. INTRODUCTION:

1.1. LITERATURE REVIEW:

1. *Steganography – A data hiding technique by Arvind kumar and pooja (2001) –* it explains that cryptography hides the content of a message while steganography conceals that a message exists at all. It discusses how text, images, audio and video can carry hidden information, the added protection of encrypting data before hiding it,

   and uses in e-commerce, secure communication and watermarking. It also covers steganalysis, which detects hidden data through unusual patterns. The study treats steganography as a security tool and does not consider its misuse to hide malware or the legal obligations of financial institutions[1].

2. *Dr. simon wiseman's report stegware – using steganography for malicious purposes(2017)*- it identifies three main uses of stegware.., compromising a device, taking data of it , and keeping up communication with it. A small hidden component, the bootstrap, triggers the concealed payload, which then runs with the user's permissions. Stegware can also bypass data loss prevention systems and use social media and file-sharing sites for covert communication. Wiseman notes that detectionbased security and sandboxing may fail and proposes Content Threat Removal, which rebuilds a clean version of a file. The report says nothing about the liability of banks, customers or payment gateways.[2]

3. *Strachanski, Petrov, Schmidbauer and Wendzel, in A Comprehensive Pattern-based Overview of Stegomalware (2024),* analyse 106 stegomalware instances from 133 reports and sort them into media-based, network-based and text-based types. Mediabased malware hides code in images such as PNGs and JPEGs through least significant bit changes, metadata editing or appended code. Network-based attacks were the most common (61 cases), followed by media-based (36) and text-based (20). Existing detection methods work only against particular techniques, so detection remains difficult. The paper does not address legal liability.[3]

[1] Arvind Kumar and Km Pooja, 'Steganography – A Data Hiding Technique' (2010) 9(7) International Journal of Computer Applications.
[2] Simon R Wiseman, Stegware – Using Steganography for Malicious Purposes, Deep Secure Technical Report DS-2017-4 (2017).
[3] Strachanski, Fabian, et al. 'A Comprehensive Pattern-Based Overview of Stegomalware'. *Proceedings of the 19th International Conference on Availability, Reliability and Security* [Vienna Austria], 2024, pp. 1–10. *DOI.org (Crossref)*, https://doi.org/10.1145/3664476.3670886.

4. *Badar, Carminati and Ferrari, in A Comprehensive Survey on Stegomalware Detection in Digital Media (2025),* discuss malware such as Zeus/Zbot, Gatak, Stegoloader and Work, which used hidden payloads to steal data and communicate secretly. They review machine learning and image steganalysis as detection methods but note that these are often format-specific, computationally expensive and weak against new techniques. Their scope is technical detection, not legal consequences.[4]

5. *Albanese and others, in StegWare: A Novel Malware Model Exploiting Payload Steganography and Dynamic Compilation (2023),* present a model in which code hidden in an ordinary image is extracted on an Android device, compiled at runtime, loaded into memory and executed. Their prototype was tested against 73 anti-malware tools, and none detected it under the study's conditions. This shows the limits of signature-based and heuristic detection. Although the study concerns Android security, it shows how hidden malware can operate without the user's awareness, which matters when assessing customer negligence and a bank's responsibility.[5]

Together, these works explain how stegware operates and why it escapes detection, but none asks who bears the loss when it is used for financial fraud. This paper takes their findings as a starting point and examines the duties of banks, the liability of customers and the reach of Indian banking and cyber law.

1.2 BACKGROUND:

India's banking industry has changed rapidly over the last decade. Banking has moved from branches and paper to internet banking, mobile applications and the unified payments interface (UPI). This has made banking faster and more accessible[6], but it has also given criminals more opportunities to divert customer's money before anyone notices.

Most banking cyber fraud discussed today involves phishing, vishing, SIM swap fraud and social engineering, where customers are deceived into revealing passwords, OTPs or PINs.

[4] Badar, Laila Tul, et al. 'A Comprehensive Survey on Stegomalware Detection in Digital Media, Research Challenges and Future Directions'. *Signal Processing*, vol. 231, June 2025, p. 109888. *DOI.org (Crossref)*, https://doi.org/10.1016/j.sigpro.2025.109888.

[5] Daniele Albanese et al., *StegWare: A Novel Malware Model Exploiting Payload Steganography and Dynamic Compilation*, *in* Proceedings of the 9th International Conference on Information Systems Security and Privacy 741, 743 (2023)

[6] India Brand Equity Foundation, Digital Banking in India: Growth, Trends & Opportunities, https://www.ibef.org/blogs/how-digital-banking-is-transforming-the-indian-banking-industry

These frauds are widely recognised, and the regulatory framework already addresses reporting and the liability of banks and customers. [7]

A less discussed threat is steganography, the technique of hiding information inside ordinary files such as images, PDFs or audio so that the file looks normal to whoever receives it. When the hidden content is malicious code, it is called stegware. An invoice, bank statement or image received by email may carry hidden code that, once the file is opened, installs malware, steals banking details or gives attackers access to the victim's system. Because the file looks genuine, customers have little reason to suspect it, and security systems that rely on known malware signatures may also miss it. [8]

This creates a legal problem. The existing approach to unauthorised transactions asks, in essence, whether the bank failed to protect its systems or the customer failed to protect credentials such as passwords, PINs or OTPs. A stegware attack fits neither category easily. A customer who opens what appears to be a genuine bank statement may not be negligent, and a bank may not have breached any clearly defined duty merely because its system missed code hidden inside a file. This paper examines these challenges, focusing on banking regulation, cybersecurity obligations and the allocation of liability between bank and customer.

1.3 STATEMENT OF THE PROBLEM:

The banking regulation act 1949, the information technology act 2000 and the RBI's cybersecurity directions require banks to adopt appropriate security measures and to prevent and respond to cyber incidents[9]. None of them specifically addresses attacks in which offenders inject malicious code into normal files through steganography, so it is unclear whether the guidelines can handle stegware. The position is more complicated where a transaction is unauthorised, because the customer liability rules were built around phishing and the theft of credentials and OTPs. In a stegware attack the customer may simply have opened a harmless looking file, and it is unclear whether the loss falls on the customer or the bank.

[7] Drishti IAS, Rising Digital Frauds and the Challenge of Ensuring Cyber Justice, https://www.drishtiias.com/daily-updates/daily-news-analysis/rising-digital-frauds-and-the-challenge-ofensuring-cyber-justice

[8] Leanne Mitton, Steganography: Hidden in Plain Sight, Splunk (Sept. 22, 2026), https://www.splunk.com/en_us/blog/learn/steganography.html

[9] Client Challenge, Scribd, https://www.scribd.com/document/813771137/Cybersecurity-in-Banking-TermPaper

1.4 RESEARCH QUESTIONS:

1. Does the Indian banking regulatory framework, including the banking regulation Act 1949, the reserve bank of india act 1934 and the directions issued under them, specifically require banks to detect or guard against stegware, or are the obligations too general?

2. If stegware leads to an unauthorised transaction, how should liability be divided among the bank, the customer and any payment gateway, and how would the RBI's 2017 circular and its judicial interpretation apply?

3. Can the UK's approach to authorised push payment fraud and the US electronic fund transfer act guide liability where neither bank nor customer can reasonably be called negligent?

4. What reforms are needed to address stegware fraud without burdening banks with detecting every technically difficult threat, while giving customers an effective remedy for losses that are not their fault?

1.5 OBJECTIVES OF THE STUDY:

- To explain how stegware works and whether current banking cybersecurity requirement can mitigate it.

- To study the Indian laws on banking cybersecurity and fraud liability, including the banking and IT statutes, RBI directions and circulars, the Bharatiya Nyaya Sanhita 2023 and the money laundering, payment systems and consumer protection laws.

- To examine judicial decisions on bank liability for unauthorised electronic transactions and their application to stegware.

- To compare india with the United Kingdom and the United States on hidden or less obvious cyber attacks.

1.6 **SCOPE AND LIMITATIONS**:

The study covers the Indian framework on banking cybersecurity and customer liability for unauthorised electronic transactions, with emphasis on image based and document based stegware. Technical detection methods are not covered, the technology is discussed only to see

whether the law can cope with it. The UK and US comparison is selective, not comprehensive. There are no reported Indian decision on steganography based banking fraud, so the paper used Indian decisions on unauthorised electronic transactions to show how courts might approach such cases.

1.7 **RESEARCH METHODOLOGY**:

The paper follows the doctrinal method, studying statues, RBI circulars and judicial decisions. The primary sources are the banking regulation Act 1949, the RBI act 1934, the Information technology Act 2000, the bharatiya Nyaya Sanhita 2023, the prevention of money laundering act 2002, the payment and settlement systems act 2007, the consumer protection act 2019 and the digital personal data protection act 2023. RBI materials include the 2017 circular on customer liability, the 2016 cyber security framework and the latest master directions on fraud risk management and digital payment security. Secondary sources include journal articles, comparative studies on UK and US banking law and technical research on stegomalware.

II. UNDERSTANDING STEGWARE: THE TECHNICAL FOUNDATION OF THE LEGAL PROBLEM:

2.1 CONCEPT AND TYPES OF STEGANOGRAPHY:

Steganography is the practice of hiding information inside an ordinary file such as an image, audio file or document, so that a person viewing it sees nothing unusual. It has legitimate uses, such as digital watermarking and copyright protection, but cybercriminals can misuse it to hide malicious data, and malicious content hidden this way is called stegware or stegomalware[10]. In banking, it could be placed in files that banks and customers exchange regularly, such as invoices, statements and transaction receipts.

There are two types of steganography: Image steganography alters pixels in ways too small for the eye to notice, or hides data in the structure of the image file.

Network steganography hides data in ordinary web traffic, for example in unused parts of network data, which lets attackers communicate secretly with compromised devices. For banks, image-based and document-based steganography are the main concern because these files

[10] *Steganography: What Is It & How Does It Work? | Okta*. https://www.okta.com/identity-101/steganography/. Accessed 4 Oct. 2026.

move constantly between banks and customers.[11]

2.2 HOW STEGWARE ATTACKS WORK:

A stegware attack usually has three stages. First, the attacker embeds malicious code in a normal file such as an image and send it to the target by email, through a website or by another route, sometimes disguised as a message from a bank. Second, once the file is opened, a separate program, which may already be on the machine or arrive at a later stage, extracts the hidden data. Third, the extracted code deploys the malware. In a banking attack, it can collect login credentials and passwords, which the attacker then uses to access accounts and make unauthorised transactions.[12]

2.3 INSTANCES OF STEGWARE IN CYBERATTACKS:

In ZeusVM, a variant of the Zeus banking trojan, the malware's encrypted configuration data was hidden in an ordinary image, which helped it locate online banking usernames and passwords while escaping standard security tools[12]. Gatak hid encoded data in an image on a genuine website, which was later used to spread malware[13]. In the Synccrypt ransomware campaign, a script downloaded an image containing malicious bits that were extracted to install ransomware[14]. ZeusVM is especially significant because it targeted online banking credentials.

2.4 DIFFICULTIES IN DETECTING STEGWARE AND THEIR RELEVANCE:

Stegware is hard to detect because the malware sits inside seemingly legitimate files. Banks cannot ignore images, PDFs, invoices and scanned documents, which are central to banking operations, and blocking them wholesale would disrupt those operations. Ordinary antivirus tools mostly look for known malware or obviously suspicious files, while stegware may show

[11] 'Types of Steganography Methods That Are Used for Hiding Confidential Data.' *DEV Community*, 8 May 2022, https://dev.to/prasan26/types-of-steganography-methods-that-are-used-for-hiding-confidential-data-1ebj.
[12] What Is Steganography?' *GeeksforGeeks*, 11 Mar. 2024, https://www.geeksforgeeks.org/cybersecurity/whatis-steganography/
[12] Paganini, Pierluigi. 'Detected New Zeus Variant Which Makes Use of Steganography'. *Security Affairs*, 18 Feb. 2014, https://securityaffairs.com/22334/uncategorized/zeus-banking-malware-nestles-crucial-file-photo.html.
[13] Catalin Cimpanu, *Keygen Websites Spreading Gatak Backdoor Trojan*, BleepingComputer (Nov. 25, 2016),
[14] Tkachenko, Eugene. 'SyncCrypt Ransomware Is Delivered in JPG Files'. *SOC Prime*, 17 Aug. 2017, https://socprime.com/news/synccrypt-ransomware-is-delivered-in-jpg-files/.

no sign of danger. Specialised tools exist, but they do not catch every attack.[15]

Customers face the same difficulty. A normal phishing attempt usually has visible warning signs, such as an odd email address or a strange link, but a document or image carrying stegware may look entirely genuine. This matters for liability, because the customer's conduct is often relevant in deciding who bears a loss. With stegware the customer may have had no realistic chance to find out that the file was harmful, and the current customer liability framework does not address malware designed to hide itself.[16]

III. LEGAL AND REGULATORY FRAMEWORK GOVERNING BANKING CYBERSECURITY IN INDIA

India has no single law on banking cybersecurity or stegware-induced fraud. Banking legislation, cyber laws, criminal laws, payment system regulation and consumer protection law each cover part of the problem, and the RBI supervises banks and issues cybersecurity directions. None specifically addresses stegware.

3.1 THE ACT 1934 AND THE BANKING REGULATION ACT 1949

The RBI Act 1934 is the legal basis for the RBI as India's central bank and gives it powers to regulate the financial system, inspect banks and act against noncompliance.[17] Section 35A of the Banking Regulation Act 1949 empowers the RBI to issue directions to banking companies in the public interest, in the interest of banking policy and to prevent the affairs of a bank from being conducted in a manner harmful to depositors[18]. This is the source of the RBI's cybersecurity and fraud prevention directions.

3.2 RBI CYBERSECURITY DIRECTIONS AND CIRCULARS

The RBI's Cyber Security Framework for Banks, 2016, requires banks to have cybersecurity policies, conduct regular security assessments, monitor threats and report cyber incidents[19].

[15] 'Stegware (Steganography Malware) — Malware of the Month'. *Spanning*, 25 July 2019, https://www.spanning.com/blog/stegware-steganography-malware-malware-of-the-month/.
[16] Goud, Naveen. 'The Growing Cyber Threat of Steganography: Concealing Malicious Activity in Plain Sight'. *Cybersecurity Insiders*, 5 May 2025, https://www.cybersecurity-insiders.com/the-growing-cyber-threat-ofsteganography-concealing-malicious-activity-in-plain-sight/.
[17] AZB & Partners, Banking Regulation in India: Overview, https://www.azbpartners.com/bank/bankingregulation-in-india-overview/
[18] Banking Regulation Act, No. 10 of 1949, § 35A (India), https://indiankanoon.org/doc/587034/.
[19] Reserve Bank of India, Notifications, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435

The Master Directions on Digital Payment Security Controls, 2021, set requirements for authentication, transaction security and risk management, and the Master Directions on Fraud Risk Management in Commercial Banks, 2024, require policies for preventing, identifying, investigating and reporting fraud.[20]

These measures do not identify steganography or image-based malware as a separate category of risk. A bank may have the required policies, conduct audits and follow reporting procedures, and still fail to detect stegware. It therefore has to be asked whether current measures are enough for concealed malware, and whether failing to identify such a threat can amount to a breach of regulatory obligations.

3.3 THE RBI's 2017 CIRCULAR ON CUSTOMER LIABILITY

The RBI's circular of 6 July 2017, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, clarifies the responsibilities of banks and customers according to the circumstances and how quickly the customer reports. Zero liability applies where the loss results from a deficiency or negligence of the bank, whether or not the customer reports it, and in third-party breaches where neither bank nor customer is at fault, provided the customer reports within three working days of the bank's communication. Limited liability applies to certain third-party breaches reported within four to seven working days. Full liability may arise where the loss results from the customer's negligence, such as sharing passwords, PINs or OTPs, until the transaction is reported. The burden of proving customer negligence lies on the bank, which must also give provisional credit within the prescribed period.[21]

3.4. THE 2026 AMENDMENT DIRECTIONS ON CUSTOMER LIABILITY

The RBI Amendment Directions, 2026 are relevant for the apportionment of liability in case of financial fraud using stegware as they amend the existing customerprotection guidelines for certain fraudulent electronic banking transactions. The amended guideline offers some additional protection to qualified customers and brings more certainty regarding the imposition of liability on banks, but does not specifically speak to malware hiding behind stegware.

[20] Reserve Bank of India, Notifications, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12715&Mode=0
[21] Reserve Bank of India, Notification, https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336

Consequently, questions may still arise regarding banks' cybersecurity measures; the customer's negligence in opening a malicious file; and whether the incident constitutes a third-party breach. The amendment provisions, while making the legal basis for safeguarding the customer stronger, are not enough without further clarification for adequately addressing the problem of stegware.[22]

3.5 THE INFORMATION TECHNOLOGY ACT 2000

The Information Technology Act 2000 is the main law on computer-related offences. Section 43 covers unauthorised access, downloading data without permission and introducing computer contaminants, and a malicious programme delivered through stegware may fall within it[23]. Section 66 punishes such acts when done dishonestly or fraudulently[24]. Section 66C deals with identity theft, the fraudulent use of another person's password or other unique identification feature, and may apply where stolen banking credentials are used to impersonate customers[25]. Section 43A provides compensation where a body corporate handling sensitive personal data fails to maintain reasonable security practices[26]. The Act does not, however, mention stegware or prescribe separate requirements for detecting code hidden in images or documents.

3.6 THE BHARATIYA NYAYA SANHITA 2023

The Bharatiya Nyaya Sanhita (BNS), 2023, which replaced the Indian Penal Code from 1 July 2024, may apply in several ways. Section 318 covers cheating and may apply where information obtained through stegware is used to deceive customers or banks and take money unlawfully[27]. Section 111 deals with organised crime, if its requirements are met. Section 335 addresses false documents and electronic records[28]. The BNS does not name steganography as a method of committing cybercrime, which may cause practical difficulty in investigation because the malicious content cannot be found by normal examination.

3.7 THE PREVENTION OF MONEY LAUNDERING ACT 2002 AND THE

[22] Reserve Bank of India, Press Release, https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=63146
[23] https://indiankanoon.org/doc/39800/ section 43 of information technology act 2000
[24] https://indiankanoon.org/doc/326206/ section 66 of information technology act 2000
[25] https://indiankanoon.org/doc/118912881/ section 66c of information technology act 2000
[26] https://indiankanoon.org/doc/76191164/ section 43Aof information technology act 2000
[27] Section 318 of the Bharatiya Nyaya Sanhita 2023
[28] Provisions under the Bharatiya Nyaya Sanhita 2023

PAYMENT AND SETTLEMENT ACT 2007

In a stegware attack, stolen funds may pass through several accounts before withdrawal. The Prevention of Money Laundering Act 2002 requires banks to verify customer identity, maintain records and report prescribed transactions, which helps trace funds from cyber fraud[29]. The Payment and Settlement Systems Act 2007 gives the RBI power to regulate payment systems and issue directions to operators, including for UPI[30]. Both laws mainly deal with what happens to money after a fraud, such as tracing, investigation and recovery, and not with the initial detection of stegware.

3.8 THE CONSUMER PROTECTION ACT 2019

Banking services come within the Consumer Protection Act 2019, and section 2(11) defines deficiency in service as any fault, shortcoming or inadequacy in the way a service is provided[31]. A customer defrauded through stegware may seek relief where the bank failed to follow the required security measures or did not respond properly to a report of an unauthorised transaction. The occurrence of a stegware attack does not itself make the bank responsible, and the commission must examine the facts and the bank's conduct. The Act offers an additional remedy where deficiency can be shown, although it does not mention stegware.

3.9 THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

The Digital Personal Data Protection Act 2023 becomes relevant when a stegware attack compromises customer data held by a bank. It requires reasonable security safeguards against personal data breaches and contains provisions on breach notification, and the Digital Personal Data Protection Rules 2025[32] add details on implementation, including phased commencement. A bank's compliance may be considered in deciding whether proper safeguards were maintained, but the Act is concerned with data protection and not with allocating liability for every unauthorised banking transaction.[33]

---

[29] *PMLA India: Requirements, Penalties & Who Must Comply | FluxForce*. 29 May 2026, https://www.fluxforce.ai/regulations/rbi-pmla-2002.
[30] https://vajiramandravi.com/upsc-exam/payment-and-settlement-systems-act-2007/.
[31] Section 2(11) of consumer protection act
[32] https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025gDOxUjMtQWa
[33] The Digital Personal Data Protection Bill, 2023'. *PRS Legislative Research*, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.

3.10 APPLICATION OF THE EXISTING FRAMEWORK TO STEGWARE

None of these laws specifically deals with malicious content hidden in ordinary files, although their provisions may still apply to stegware depending on the facts of the attack. The real concern is whether the framework is sufficient when the attack stays hidden from both bank and customer. Liability then depends on the bank's security measures, the customer's precautions and the circumstances of the transaction, which the next section examines.

IV. LIABILITY ALLOCATION IN STEGWARE-INDUCED FRAUD: BANKS, CUSTOMERS AND PAYMENT GATEWAYS

4.1 THE CONTRACTUAL AND FIDUCIARY NATURE OF THE BANK-CUSTOMER RELATIONSHIP

The relationship between a bank and its customer is primarily contractual and begins when an account is opened, but it also places a duty of care on the bank. In *Canara Bank v. Canara Sales Corporation & Ors.*, the Supreme Court held that banks must exercise a high degree of care in managing customer accounts and may be liable for negligence in handling transactions.[34] In *State Bank of India v. Shyama Devi*, the Court held that a bank can be responsible for the acts of its employees done in the course of employment.[35] These cases did not involve digital banking, but their principles still apply: customers depend on the bank's security systems, so the bank must take reasonable steps to protect their accounts.

4.2 JUDICIAL APPROACH TO BANK LIABILITY IN UNAUTHORISED ELECTRONIC TRANSACTIONS

In *Umashankar Sivasubramanian v. ICICI Bank*, the National Consumer Disputes Redressal Commission held the bank liable for unauthorised credit card transactions made without the customer's knowledge. It held that customers should not bear losses caused by a bank's failure to maintain proper security, and that the bank must show adequate security systems were in place.[36] In *ICICI Bank Ltd. v. Shanti Devi Sharma*, the forum held that failure to provide secure ATM facilities was a deficiency in service, showing that authentication by password or PIN

[34] Canara Bank v. Canara Sales Corp. & Ors., AIR 1987 SC 1603.
[35] State Bank of India v. Shyama Devi, AIR 1978 SC 1263.
[36] Umashankar Sivasubramanian v. ICICI Bank, NCDRC (2010).

does not by itself prove that the bank met its duty of care.[37]

The Supreme Court has also recognised that consumer forums may not suit every complex fraud dispute. In *Oriental Insurance Co. Ltd. v. Munimahesh Patel*, it pointed to the limits of summary proceedings where complicated facts need detailed examination.[38] This matters for stegware, because establishing how the malware entered a system, whether it caused the transaction and whether the bank's security was adequate may need technical investigation and expert evidence, for which a competent court may be more suitable. These decisions show that a bank's liability depends on the facts, and because stegware is concealed, liability requires examining the bank's measures, the customer's conduct and the circumstances of the transaction.

4.3 APPLYING THE RBI's ZERO, LIMITED AND FULL LIABILITY FRAMEWORK

The 2017 circular broadly considers three situations: a transaction caused by the bank's negligence, a third-party breach where neither bank nor customer is responsible, and a transaction resulting from the customer's negligence. Since stegware hides malicious code in ordinary-looking files, it may be difficult to tell which of these applies.

(a) Whether stegware-induced fraud amounts to a bank deficiency

A bank may argue that it met its obligations through regular audits, antivirus and endpoint protection and approved cybersecurity policies, and that failure to detect stegware is not a deficiency in service. As Part III showed, conventional tools are not designed to catch concealed threats, and even specialised tools are unreliable. At the same time, *Umashankar Sivasubramanian case* suggests that banks may still have to show that their security was adequate[40], and a bank that cannot do so may be held liable. The law does not currently say how adequacy should be weighed against the nature of the attack.

(b) Whether stegware-induced fraud amounts to an unattributable third-party breach

This appears to be the closest fit for many stegware attacks. The fraud is carried out by an external attacker without negligence by the bank or the customer, and the code may be hidden in a document or image that neither could identify. Under the 2017 circular, the customer then

[37] ICICI Bank Ltd. v. Shanti Devi Sharma, Consumer Forum (2008).
[38] Oriental Insurance Co. Ltd. v. Munimahesh Patel, (2006) 7 SCC 655.

has zero liability if the transaction is reported within three working days. However, some stegware attacks run in the background for a long time before any unauthorised debit appears. The customer may discover the fraud only after the reporting period has passed, which could increase their liability even though the delay was not caused by their negligence.

(c) Whether stegware-induced fraud amounts to customer negligence

This category places the greatest burden on the customer, and a bank may argue that the customer should not have opened an unsolicited attachment or downloaded a file from an untrusted source. But sharing an OTP or clicking a link in an obviously fraudulent email is very different from opening a document that looks genuine and forms part of an ordinary banking transaction. A stegware file may seem safe to an ordinary user, and even the customer's security software may miss it. Simply opening it should not automatically count as negligence. The question should be whether the risk was reasonably identifiable and whether the customer failed to take precautions that could reasonably have been expected.

Overall, the RBI framework does not clearly address stegware. Classifying it as an unattributable third-party breach may often protect customers best, but the circular does not expressly guarantee this, the reporting period may be unfair where malware stays undetected for long, and banks may still invoke customer negligence. This uncertainty shows the need for a framework better suited to stegware-related fraud.

4.4 THE POSITION OF PAYMENT GATEWAYS AND INTERMEDIARIES

Stolen funds may pass through payment gateways or other intermediaries, including UPI platforms. Section 79 of the Information Technology Act 2000 gives intermediaries conditional protection from liability for third-party information on their platforms, subject to due diligence[39]. This protection was developed mainly for intermediaries that host or transmit third-party content, and its application to payment intermediaries that process fraudulent transfers is less certain.

A payment gateway is neither the customer whose account was compromised nor the bank whose systems may have been affected. Its responsibility must be assessed separately under its own legal obligations, including those under the Payment and Settlement Systems Act 2007.

[39] Section 79 of the Information Technology Act 2000

Its involvement does not remove or replace the liability of the bank or the customer and should be treated as an additional part of the overall liability framework.

V. COMPARATIVE PERSPECTIVES

5.1 The United Kingdom: Mandatory Reimbursement for Authorised Push Payment Fraud

Authorised push payment (APP) fraud occurs when a customer is deceived into voluntarily sending money to a fraudster. Since October 2024, the United Kingdom has required banks and other payment service providers to reimburse most eligible victims, subject to exceptions and a maximum claim of £85,000. Sending and receiving institutions share the cost, and refunds must generally be made within five business days. It matters for stegware because it does not make the bank's negligence the only basis for compensation. It accepts that some frauds cause loss even where the customer's actions appear to authorise the payment, and by sharing the cost it places part of the burden on the payment system instead of leaving the whole loss with the victim.[40]

5.2 The United States: The Electronic Fund Transfer Act

Under the Electronic Fund Transfer Act (EFTA) and Regulation E, a customer's liability for unauthorised electronic fund transfers depends on how quickly the loss is reported. It is generally limited to $50 if reported within two business days, and may rise to $500 if reported after that but within 60 days of the account statement. After 60 days, the customer may be liable for further losses.

These protections mainly apply to transactions the customer did not authorise, and protection is more limited where the customer is deceived into willingly making a transfer. In stegware cases, malicious software may manipulate a genuine banking session so that a transaction looks authorised although the customer was unaware of the fraud, and recovery may then depend on the bank's voluntary reimbursement policy. This resembles India's position, where the line

[40] 'The U.K.'s Authorised Push Payment (APP) Fraud Reimbursement Scheme'. *A&O Shearman*, https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/the-uks-authorisedpush-payment-app-fraud-reimbursement-scheme.

between authorised and unauthorised transactions affects liability.[41]

5.3 Lessons for India

Both systems show the importance of distinguishing genuinely authorised transactions from those that happen through fraud or deception. A framework based entirely on proving negligence may leave customers without adequate protection when neither party's fault can be established. The UK model suggests a system of shared liability and reimbursement for certain sophisticated electronic frauds, which could reduce disputes over whether a transaction was technically authorised and give clearer rules for sharing losses among banks, customers and payment service providers. It would still have to account for the conduct of the parties and existing safeguards.

VI. CONCLUSION

This study finds that India's existing banking and cyber laws provide a general basis for addressing financial fraud but are insufficient to deal with the specific challenges of stegware-induced fraud. The analysis reveals that the existing RBI framework largely depends on customer negligence, prompt reporting and the distinction between authorised and unauthorised transactions. However, where concealed malware operates without the customer's knowledge or deliberate disclosure of credentials, determining liability becomes difficult. The study further identifies the need to examine the security obligations of banks and the role of payment intermediaries rather than placing the entire responsibility on customers. The comparative analysis of the United Kingdom and the United States demonstrates the importance of clearer consumer protection and liability allocation. Therefore, India requires specific guidelines addressing concealed malware attacks, including a fair mechanism for allocating losses where neither the customer nor the bank is directly at fault.

VII. FINDINGS:

1. Currently, there is no clear legal duty on banks on stealware or malware which is based on steganography: as mandated in the Reserve Bank of India Act, the Banking Regulation Act, or the RBI's cybersecurity guidelines in 2016, 2021 and the upcoming 2024 Master Directions.

[41] 'Electronic Fund Transfer Act'. *Wikipedia*, 8 Apr. 2025. *Wikipedia*, https://en.wikipedia.org/w/index.php?title=Electronic_Fund_Transfer_Act&oldid=1284525602.

Apart from this, the legal duties are related to minimum security standards in place but do not directly refer to the use of stegosystems/image-based malware.

2. Cyber Laws: The IT Act and BNS Act IT Act and BNS Act are unlikely to directly govern stegware, but might do so in a certain sense. Under the IT Act, sections 43, 66 and 66C, as well as sections 318, 111 and 335 in the BNS, could theoretically include stegware fraud depending on the context. The concept of steganography does not formally appear in either statute as a means of a cybercrime.

3. The RBI's 2017 circular does not seem very effective for dealing with riskware. It condemns breaches of unauthorised third parties with no accountability for customers. But it doesn't even clearly state that customers will be treated as such, and the three-day deadline may put customers at a disadvantage, with malware being latent for a while.

4. A bank's liability hinges on whether its security was sufficient. The study by Umashankar Sivasubramanian and Shanti Devi Sharma says that while the burden of proof is on the bank, it is unclear as to how adequacy could be proved with respect to a secret attack. In addition, consumer forums are simply not well-equipped to deal with disputes of this technical nature, says Munimahesh Patel.

5. The liability of the payment gateways remains unknown. Initially, sec 79 was meant for content intermediaries, and how it applicable to payment intermediaries is not clear.

6. The UK model might be a good fit. It would require reimbursement shared liability and not test for negligence. The US model, which is the Electronic Fund Transfer Act (EFTA) model, relies on authorization and reporting time frames for transactions to determine reimbursement which may not work for stegware.

VIII. SUGGESTIONS / RECOMMENDATIONS:

The following recommendations aim to close the gaps in India's framework on stegware-induced financial fraud.

1. Clarify customer liability. The RBI should expressly classify losses caused by malware concealed through steganography as third-party breaches where the customer could not reasonably have detected the threat. This would ensure zero liability where the customer

was not negligent.

2. Extend the reporting period. The period for zero-liability protection should run from the date on which the customer discovers, or could reasonably have discovered, the fraud. This would protect customers from hidden attacks that stay undetected for some time.

3. Strengthen banks' cybersecurity obligations. The RBI should set clear requirements for detecting concealed malware, including suitable steganalysis measures for banks handling high volumes of digital transactions, so that the standards for preventing such attacks are specific and measurable.

4. Improve reporting and investigation. The National Cyber Crime Reporting Portal should have a separate category for stegware-related fraud, and cyber forensic laboratories should be equipped with suitable tools and trained personnel to investigate such attacks.

5. Clarification of Criminal Liability. Clear prosecutorial guidelines should be established to explain the application of relevant provisions of the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 to stegware-induced financial fraud, ensuring consistent investigation, interpretation and prosecution of such offences across jurisdictions.

The paper therefore stresses the need to clarify customer liability, strengthen banks' cybersecurity obligations, improve investigation and provide clearer rules for sharing losses. The law must be able to deal with attacks designed to stay hidden and make fault hard to identify, and stegware shows why India's digital banking system needs a more specific approach to liability.