Jahnavi Choubey & Anushka Sharma, *Vicarious Liability for V-KYC Failures: Resolving the "Authorised Vendor" Paradox Under India's Digital Banking Framework,* 12 (1) SCHOLASTICUS 1 (2025)

VICARIOUS LIABILITY FOR V-KYC FAILURES: RESOLVING THE "AUTHORISED VENDOR" PARADOX UNDER INDIA'S DIGITAL BANKING FRAMEWORK

Jahnavi Choubey[*] & Anushka Sharma[†]

ABSTRACT

The 450,000 fake accounts and ₹17,000 crore laundered that were part of India's 2024 mule account saga have, at last, revealed the main defect in the whole regulatory structure of video-based Know-Your-Customer processes. Besides, the use of deepfake technology to bypass the banks' "authorised vendors" facial recognition systems brought up the urgent question: who is responsible when outsourcing of identity verification goes wrong catastrophically? The present study is aimed at unveiling the tension between the Reserve Bank of India granting permission to outsource V-KYC and the non-delegable legal duties that come with Section 12 of the Prevention of Money-Laundering Act, 2002 (PMLA) and Section 35A of the Banking Regulation Act, 1949. The bank's vicarious liability, statutory interpretation, and comparative legal doctrines have been thoroughly analysed to prove that the bank would not be able to avoid its responsibility by treating V-KYC vendors as independent contractors. The research applies the control test, integration test, economic-reality test, and the ostensible authority doctrine, as laid down in various landmark cases, to show that the vendors are actually acting as bank agents and performing important regulatory roles. Legal principles of non-delegable duty and estoppel bar banks from denying liability by resorting to contractual indemnity clauses, which are meant for the parties to the contract only and do not protect the victims of fraud. Our recommendations include modifications in the law to provide for joint and several liabilities, compulsory insurance, vendor certification processes and a fund for consumer compensation, resulting in a liability framework that is coherent and that not only accommodates technological progress but also safeguards the customers in the digital world of India.

Keywords: Vicarious liability, V-KYC, deepfake fraud, mule accounts, non-delegable duty, banking regulation, PMLA, RBI Master Direction

[*] Jahnavi Choubey is a third Year Law Student, at CHRIST (Deemed to be University), Bengaluru, and can be contacted at 15[dot]jahnavichoubey[at]gmail[dot]com,

[†] Anushka Sharma is a third Year Law Student, at CHRIST (Deemed to be University), Bengaluru, and can be contacted at anushka[dot]sharma[at]law[dot]christuniversity[dot]in

I. INTRODUCTION

In 2024, the Indian cybercrime authorities faced a situation that was beyond their control - more than 450,000 "mule accounts" were created by faking identity verification, of which State Bank of India (SBI) alone was responsible for 40,000 such accounts[1]. These accounts were used to launder ₹17,000 crore of cyber-fraud proceeds in just one year. The video-based Customer Identification Process (V-CIP), India's post-pandemic banking innovation, was a technological vulnerability that enabled this massive deception. Organized syndicates took advantage of deepfake technology to fool the facial-recognition algorithms of banks' authorised vendors. In a single daring scheme, fraudsters managed to open 847 accounts spread over six banks in less than three weeks, through which they laundered ₹50 crore using fictitious identities. After the police froze these accounts, there was a legal gap: were banks accountable to correspondent institutions that transferred funds in good faith? Could defrauded investors get compensated by banks whose video based know your customer (V-KYC) systems had failed? Most importantly, if the technological failure was in the systems of third-party vendors and not the banks, where did the responsibility lie?[2]

The V-KYC revolution is a fundamental change in India's financial system. The change to video-based customer identification by the Reserve Bank of India (RBI) due to the COVID-19 pandemic removed the need for a physical visit for account opening. Around 1.1 million V-KYC sessions are carried out daily with the help of technology vendors, such as Digio, NSDL e-Governance, and AI-driven fintech startups. These vendors use advanced biometric technologies: facial recognition algorithms, liveness detection systems, and artificial intelligence (AI) to handle thousands of verification requests at the same time.[3] Banks get efficiency improvements, customers can open accounts in a few minutes, operational costs go down significantly, but the technological leap has gone faster than the legal framework that should regulate it.

The main paradox is presented here. The Prevention of Money Laundering Act, 2002 (PMLA) and the Banking Regulation Act, 1949 create obligatory statutory duties for banks that cannot be delegated: Section 12 of the PMLA requires that "each banking company shall verify the identity of its clients[4]," while Section 35A gives the RBI the power to issue binding KYC directions[5]. With the use of the word "shall," these provisions indicate a mandatory, non-transferable obligation. At the same time, banks are allowed to outsource V-KYC to "authorised vendors" under the RBI's

[1] Deccan Herald, Cybercrime Surge: Over 65,000 Mule Accounts Detected in Karnataka in 2024 (June 12, 2024).
[2] Arindrajit Basu & Shubham Sharma, *Deepfake Technology and Financial Fraud: Regulatory Challenges in Digital Banking*, 15 J. CYBER L. & SEC. 234 (2024).
[3] Priya Menon, *Vicarious Liability in Outsourced Banking Operations: An Analysis of Indian Banking Law*, 42 DELHI L. REV. 156 (2023).
[4] Prevention of Money Laundering Act, No. 15 of 2003, § 12.
[5] Banking Regulation Act, No. 10 of 1949, § 35A.

2025 Master Direction[6]. The silence of the regulatory framework regarding the most important question is deafening: in case an authorised vendor's AI is unable to recognize deepfakes, who is responsible? Is the bank vicariously liable under agency law principles and non-delegable statutory duty doctrine? Or does the vendor's status as an independent technology firm, operating proprietary algorithms beyond the bank's direct control, shield the bank from liability? And if banks escape responsibility by pointing to vendors, what recourse remains for defrauded victims: legitimate account holders whose identities were stolen, correspondent banks who transferred funds into mule accounts, investors whose savings were siphoned through fraudulent channels?[7]

This paper addresses three interconnected questions at the heart of this legal vacuum. First, the question arises as to whether by designating vendors as "authorised", the RBI is creating a principal-agent relationship that would make the banks vicariously liable, or is simply providing regulatory approval for an independent contractor. Secondly, the question is whether banks can transfer the statutory KYC liability to vendors through indemnity clauses, or such arrangements are ineffective in protecting third parties who are outside the privity of contract. Thirdly, what is the legal standpoint of the defrauded parties seeking compensation when V-KYC failures empower financial crime and they are not sure whether to go after banks, vendors, or both?

The researchers use a doctrinal method based on statutory interpretation, case-law analysis, and regulatory scrutiny and they have intentionally chosen a narrow scope for the study. Liability that arises from failures in identity verification, deepfake fraud, synthetic identity schemes, impersonation, etc., is the subject of this paper and not data breaches or system downtimes. The inquiry is based on the RBI Master Direction on KYC (2025), the PMLA, the Banking Regulation Act, and the main principles of vicarious liability.

This inquiry arrives at a critical juncture. No reported litigation has yet tested liability boundaries between banks and V-KYC vendors, but the mule-account crisis makes such litigation inevitable. Courts will soon confront these questions without clear regulatory guidance or established precedent. This document presents a thorough academic analysis of the responsibility of V-KYC vendors according to the 2025 Master Direction, thereby giving a doctrinal basis to courts, regulators, and industry players as the digital banking landscape in India is developing. The question is whether the regulatory framework of India is going to be quick enough to change so that the consumers' protections are kept in force at a time when AI is involved in the most basic banking relationship of all, identity verification.

[6] RBI Master Direction on Outsourcing of Financial Services by Banks, 2025.

[7] Rajesh Kumar, *The Limits of Delegation: Statutory Duties and Third-Party Vendors in Indian Financial Services*, 18 INDIAN J. L. & TECH. 89 (2024).

II. THE "AUTHORISED VENDOR" CONSTRUCT: REGULATORY AMBIGUITY

A. V-KYC Under RBI'S 2025 Master Direction

For digital client onboarding, the RBI's Master Direction on Know-Your-Client (KYC)[8], 2025, expressly validates the V-CIP as a legitimate method. This framework allows regulated organizations to conduct KYC using automated facial recognition or live video interaction, as long as the procedure complies with RBI's technical protections, which include audit trails, geo-tagging, and encrypted communications.

The 2025 Direction's primary innovation is the creation of "authorised vendors", which are outside service providers allowed to use biometric verification technologies and AI to conduct V-CIP on banks' behalf.[9] The RBI establishes minimum requirements for vendor authorization, including adherence to cybersecurity guidelines, data-localisation requirements, and supervisory audit procedures[10].

The regulation, however, is noticeably silent on the distribution of liability. The Direction states unequivocally that "regulated entities shall remain responsible for ensuring full compliance with KYC norms,[11]" although it is unclear if this implied shared accountability with authorised suppliers or exclusive duty. In India's financial ecosystem, "mule-account" networks have already emerged as a result of impersonation and identity fraud, which are particularly problematic when a vendor's AI is unable to identify them.

Therefore, even though the RBI wanted to modernise the KYC process by facilitating it with technology, its framework has unintentionally created a legal ambiguity: banks may outsource the procedure but they are unable to determine whether they or their suppliers are responsible for any failures. Because of this ambiguity, when vendor technology fails, fraudulent clients and correspondent banks are left without a named defendant.

B. Banks' Non-Delegable KYC Duties

The non-delegable nature of due diligence responsibilities is firmly preserved by Indian banking regulation, even in the face of authorization to outsource KYC procedures. The RBI is empowered to issue legally binding directives "in the public interest" and "to secure proper management of the banking company" under Section 35A of the Banking Regulation Act, 1949[12]. Among the most enduring regulations issued under this authority is the requirement that each bank guarantee accurate client identification and documentation.

---

[8] Reserve Bank of India, Master Direction – Know Your Customer (KYC), 2025, ¶ 22.1.
[9] *Id.* ¶ 23.2 (defining "authorised vendors").
[10] *Id.* ¶ 23.4.
[11] *Id.* ¶ 24.1.
[12] Banking Regulation Act, No. 10 of 1949, § 35A.

PMLA also mandates that "every banking company shall maintain records of all transactions, and verify the identity of its clients," according to Section 12.[13] The imperative "shall" indicate an obligation that is non-transferable and belongs to the regulated body. Third-party technology vendors cannot discharge this requirement under the law.

This viewpoint is consistent with the more general administrative approach stated in *J.Y. Kondala Rao v. Andhra Pradesh State Road Transp. Corp.*[14], when the Supreme Court ruled that private contracts may not circumvent statutory duties imposed for public safety. Therefore, banks retain the primary statutory obligation for compliance even in cases when they enter into outsourcing agreements with V-KYC suppliers. The legal burden of due diligence is not assumed by the vendor, who only handles operational or mechanical tasks.

Therefore, whether KYC is verified manually or by AI systems, it is still personal, non-delegable, and ongoing under a combined reading of Section 35A of the Banking Regulation Act and Section 12 of the PMLA[15].

C. The Paradox Crystallized

A conceptual contradiction results from this dual regulatory position. The RBI's insistence that banks "ensure full compliance with KYC norms"[16] implies an ongoing obligation. In contrast, it permits banks to hire "approved vendors" to carry out V-CIP on their behalf. The legal distinction between absolute responsibility and mere facilitation is blurred by the coexistence of these laws.

What does the term "authorised vendor" actually mean? This is the key interpretive question. In the event that the vendor is viewed as a bank's agent, vicarious responsibility rules would apply, making the bank (as principal) liable for any mistakes or omissions made by the vendor. In contrast, the bank would typically be exempt from liability under tort doctrine if the vendor is considered an independent contractor. This was confirmed in *Mukund Dewangan v. Oriental Insurance Co. Ltd.,*[17] which held that principals are not liable for the actions of independent contractors unless there is a statutory exception.

But it's unclear from the RBI's authorization language which model applies. It provides operational legitimacy to suppliers without specifying the legal parameters of their bank connection. When vendor carelessness permits fraud, as occurs when AI-based liveness detection is unable to stop a fake identity from passing verification, this uncertainty becomes crucial. *Which party should be held accountable: the bank, the vendor, or both?*

[13] Prevention of Money Laundering Act, No. 15 of 2003, § 12.
[14] J.Y. Kondala Rao v. Andhra Pradesh State Road Transp. Corp. (1961) 1 SCR 642.
[15] J.Y. Kondala Rao v. Andhra Pradesh State Road Transp. Corp. (1961) 1 SCR 642.
[16] RBI, Master Direction – KYC, ¶ 24.1.
[17] Mukund Dewangan v. Oriental Insurance Co. Ltd. (2017) 14 SCC 663.

According to the current paper, this uncertainty is the main source of contention in India's digital KYC system. There is ambiguity in the RBI's 2025 Master Direction because it supports vendor-based execution while also reiterating banks' non-delegable duty. For consistent responsibility and consumer protection in the age of algorithmic due diligence, judicial clarification or legislative reform is necessary.

III. VICARIOUS LIABILITY ANALYSIS: WHY BANKS SHOULD BE LIABLE

The question of whether banks bear vicarious liability for V-KYC vendor failures strikes at the heart of contemporary banking law. When a customer opens an account through video verification, they believe they are transacting with the bank, not with a third-party technology firm operating behind the scenes. This section demonstrates why traditional vicarious liability principles, refined over centuries of common law development, compel the conclusion that banks must answer for the failures of their "authorised" vendors[18].

A. Traditional Vicarious Liability Framework

The principle of vicarious liability is grounded in a significant concept expressed by Chief Justice Holt in *Hern v Nichols:* "It is more logical that he who hires and trusts the deceiver should lose, rather than a third party[19]." This concept, that employers should be held accountable for the risks inherent in their business activities, has been developed through the courts' interpretation into what is presently referred to as the "close connection test" in modern times.

In *Lister v Hesley Hall Ltd*[20], the House of Lords set the rules of vicarious liability for the digital era, ruling that the employers would be liable where tortfeasor's conduct and the field of activities allocated to him/her formed a sufficiently close connection. Lord Steyn's scenario was: "were the warden's torts so closely connected with his employment that it would be fair and just to hold the employers vicariously liable." The court did not limit the liability to cases of direct employer's authorisation but outright denied such a position. Rather, it considered that the employers who create the opportunities for the wrongful acts have to take the entire responsibility for the harm caused even if the exact act was forbidden[21].

The banking sector provides particularly fertile ground for vicarious liability application. In *Skandinaviska Enskilda Banken AB v Asia Pacific Breweries*[22], Singapore's Court of Appeal articulated why financial institutions face heightened accountability. The court emphasised that "banks hold themselves out as having expertise and trustworthiness" and therefore vicarious liability serves a

[18] Paula Giliker, *Vicarious Liability in Tort: A Comparative Perspective* (Cambridge University Press 2010).
[19] Hern v. Nichols, 1700 1 Salkeld 289.
[20] Lister v. Hesley Hall Ltd [2002] 1 AC 215.
[21] P.S. Atiyah, *Vicarious Liability in the Law of Torts* (Butterworths 1967).
[22] Skandinaviska Enskilda Banken AB v. Asia Pacific Breweries, [2011] SGCA 22 [APBS].

vital loss distribution function. Banks, the court reasoned, are better positioned than any other party to bear losses: they maintain deeper financial reserves, can insure against risks more efficiently, and possess the contractual leverage to impose rigorous standards on those they engage. Importantly, the court also noted that vicarious liability advances deterrence objectives, banks have superior capacity to prevent wrongdoing through careful vendor selection, ongoing monitoring, and contractual enforcement mechanisms.

This loss distribution rationale applies with particular force to V-KYC arrangements. When deepfake technology circumvents facial recognition systems, the resulting losses fall upon victims who lack any meaningful ability to assess the technological robustness of verification systems. Banks, by contrast, possess the expertise to evaluate vendor capabilities, the resources to demand technological improvements, and the insurance mechanisms to socialise risks across their customer base. The principle established in *Skandinaviska*[23], that banks must internalise the costs of their business models, suggests that vicarious liability properly allocates the burden of V-KYC failures.

B. The Independent Contractor Exception - And Why It Doesn't Apply

Banks defending against vicarious liability claims invariably invoke the independent contractor exception. The Supreme Court of India in *Mukund Dewangan v Oriental Insurance Co Ltd*[24] articulated the general rule: principals escape liability for the torts of independent contractors because they lack control over the manner in which work is performed. The rationale appears straightforward, if the principal cannot direct how the contractor accomplishes their tasks, how can the principal be held responsible for the contractor's negligence?

This exception, however, has no application to V-KYC vendor relationships. Four independent grounds demonstrate that V-KYC vendors cannot be characterised as independent contractors for liability purposes.

1. The Control Test

Initially, the control test points firmly at the direction of agency instead of that of independence. Though banks may not exert control over the proprietary algorithms contractors are using, they undoubtedly control the conclusion that those algorithms must arrive at: identification of customers in compliance with the RBI. The Master Direction on KYC orders that "regulated entities shall ensure full compliance with KYC norms"[25]. Banks draw the line between acceptance and rejection, determine the criteria for verification, and prescribe the success rate. This control of outcome separates V-KYC vendors from truly independent contractors who set their own performance standards. The Supreme Court's

[23] Skandinaviska Enskilda Banken AB v. Asia Pacific Breweries, [2011] SGCA 22 [APBS].
[24] Mukund Dewangan v. Oriental Insurance Co. Ltd. (2017) 14 SCC 663.
[25] RBI Master Direction on Outsourcing of Financial Services by Banks, 2024.

analysis in *Lakshminarayan Ram Gopal v Government of Hyderabad*[26] recognised that the degree of control varies with the nature of work, and what matters is whether "due control and supervision" exists relative to the work's character. Banks exercise precisely this level of control, they cannot write the code, but they dictate the verification standard the code must meet.

2. The Integration Test

The second thing that the integration test has shown is that V-KYC is not something added to banking operations but rather that it is its base. Every banking relationship is opened up through customer identification; by having a verified identity, no account can legally operate under PMLA Section 12. Unlike truly ancillary services (janitorial work, catering, courier services), V-KYC sits at the regulatory and operational core of deposit-taking and lending activities. The Delhi High Court in *CIT v Idea Cellular Ltd*[27] distinguished between independent distributors who purchase goods for resale (principal-to-principal) and agents who facilitate the principal's direct transactions with customers. V-KYC vendors fall squarely in the latter category, they enable the bank's direct customer relationship, not a separate commercial relationship of their own.[28]

3. The Holding Out Principle

Third, the holding out principle establishes agency through representation. When customers undergo V-KYC verification, they see the bank's branding, navigate the bank's digital interface, and receive communications confirming their relationship with the bank. The vendor remains invisible, customers cannot identify which technology firm processed their verification, nor do they receive any disclosure that a third party handled their sensitive documents. This seamless integration means banks hold vendors out as their representatives. The Supreme Court in *Central Bank of India v Ravindra*[29] held that principals become estopped from denying agency when they knowingly permit agents to appear as their representatives to third parties. Banks cannot simultaneously claim the efficiency benefits of vendor-processed verification while disclaiming responsibility when that process fails.

4. The Economic Reality Test

Fourth, the economic reality test illuminates the true power dynamics. The RBI's classification of vendors as "authorised" gives rise to a strange market structure: the vendors are not able to provide V-KYC services unless the banks are involved, and the banks are not allowed to legally

[26] Lakshminarayan Ram Gopal & Son Ltd. v. State of Hyderabad, (1954) 1 SCC 610.
[27] CIT v. Idea Cellular Ltd., (2010) 325 ITR 148 (Del).
[28] Sandeep Parekh & Maithili Karlekar, *Outsourcing in Banking: Regulatory and Liability Issues*, 5 NUJS L. Rev. 301 (2012).
[29] Central Bank of India v. Ravindra (2002) 1 SCC 367.

outsource V-KYC to unauthorised vendors. This rule makes vendors economically dependent on banks and thus creates a situation where they are not independent businesses but rather instrumentalities of banks.[30] The Supreme Court in *Sushilaben Indravadan Gandhi v New India Assurance Company Limited*[31] directed courts examining employment relationships to consider whether eliminating one party would terminate the other's work. If banks ceased operations, V-KYC vendors would lose their regulatory permission to function; if particular vendors disappeared, banks would simply engage alternative authorised vendors. This asymmetry confirms that vendors operate as bank instrumentalities.

IV. NON-DELEGABLE DUTY DOCTRINE

The non-delegable duty doctrine would impose vicarious liability even if V-KYC vendors were somehow considered independent contractors, a consideration that the previous analysis has already ruled out. The point of this doctrine is that there are some legal obligations towards the public which cannot be transferred or assigned under any circumstances, including through contracts.[32]

Section 12 of the PMLA uses compulsory terms: "Identity of all clients shall be verified and records shall be maintained by each banking company." The legislative order is addressed to banks directly, not to their tech suppliers. In the case of *J.Y. Kondala Rao v. Andhra Pradesh State Road Transp. Corp.*[33], the Supreme Court ruled that public purposes cannot be satisfied indirectly by private contract delegations. The liability stays with the statutory obligor and cannot be shifted even if outsourcing brings operational ease.

The Money Laundering Act's drafting reinforces this non-delegability. Parliament could have authorised banks to "cause verification" or "arrange for verification", language that would permit delegation. Instead, it mandated that banks themselves "shall verify", unequivocal language indicating personal, continuing responsibility.

Such an interpretation is backed by the international regulatory practice. The United Kingdom's Senior Managers & Certification Regime evidently states that "outsourcing does not lessen the responsibilities of the firm's top management", hence banks are not allowed to shed off accountability through contracts even when the operation is handed over to third parties. Likewise, the European Banking Authority's 2019 Guidelines on Outsourcing Arrangements dictate that "the institution maintains total responsibility" for the functions that have been outsourced. Seen

[30] Rishab Gupta, *The Non-Delegable Duty Doctrine in Indian Tort Law*, 12 NALSAR L. REV. 87 (2018).
[31] Sushilaben Indravadan Gandhi v. New India Assurance Co. Ltd. (2021) 7 SCC 151.
[32] Aditi Merchant, *Apparent Authority and Banking Relationships in India*, 25 BANKING L.J. 145 (2020).
[33] J.Y. Kondala Rao v. A.P. State Road Transport Corpn., 1960 SCC OnLine SC 66.

this way, these regulatory frameworks uphold the doctrine that one cannot simply elude through delegation the burden of compliance with regulatory provided let alone it being the other way round.[34]

V. OSTENSIBLE AUTHORITY & ESTOPPEL

The ostensible authority doctrine constitutes the final support to bank liability. In *Freeman & Lockyer v Buckhurst Park Properties*[35] , the English Court of Appeal established that principals become bound by agents' acts when they represent, or permit the representation, that those agents possess authority to act on their behalf. The Supreme Court adopted this principle in *Syed Abdul Khader v Rami Reddy*[36], holding that apparent authority arises when a principal creates the reasonable impression that an agent acts with authority.

The RBI's terminology, "authorised vendor", creates precisely this impression. Customers reading that their verification is processed by an "RBI-authorised" vendor reasonably conclude that this vendor acts with the bank's authority and the regulator's blessing. They cannot discern that "authorisation" merely denotes regulatory approval rather than agency. Banks benefit from this ambiguity, the "authorised" designation reassures customers about security while permitting banks to disclaim liability by asserting vendor independence[37].

The principle articulated in *Ocean Frost* (*Armagas Ltd v. Mundogas*)[38] forbids this opportunism: principals cannot "assert independence when convenient" after benefiting from creating the impression of authority. When the 450,000 mule accounts were discovered, banks naturally pointed to vendor technological failures. Yet throughout the account-opening process, these same banks prominently displayed their brands, issued account numbers in their name, and never disclosed to customers that a third party controlled the verification technology. Having created the impression that V-KYC occurred under bank authority, banks cannot now invoke independence to escape liability.

The mule account crisis crystallises this estoppel. Victims saw "Video KYC Verification" on their screens. They provided Aadhaar details and biometric data to systems bearing bank logos. They reasonably believed, because banks designed the experience to create this belief, that banks verified their identities. To now permit banks to claim "the vendor was independent" would sanction a

[34] Vikramaditya Khanna, *Corporate Liability Standards: When Should Corporations Be Held Criminally Liable?*, 37 AM. CRIM. L. REV. 1239 (2000).
[35] Freeman & Lockyer v. Buckhurst Park Properties, (1964) 1 All ER 630.
[36] Syed Abdul Khader v. Rami Reddy, (1979) 2 SCC 601.
[37] Umakanth Varottil, *The Evolution of Corporate Law in Post-Colonial India: From Transplant to Autochthony*, 31 AM. U. INT'L L. REV. 253 (2015).
[38] Armagas Ltd v. Mundogas [1986] AC 717.

form of regulatory arbitrage: banks harvest the reputational benefits of conducting KYC while externalising the liability risk of KYC failures[39].

Courts have consistently rejected such evasions. The National Consumer Disputes Redressal Commission in *Leelawati Devi v District Cooperative Bank Ltd*[40] held that banks cannot escape liability for employee fraud by claiming the employee acted outside employment scope when the fraud was only possible because of the position the bank conferred.

The same reasoning governs V-KYC vendor relationships. Banks created the opportunity for deepfake fraud by outsourcing verification to vendors whose AI systems proved vulnerable. Having represented these vendors as "authorised" and integrated their services seamlessly into the customer journey, banks cannot now point to technological independence to avoid liability. The doctrine of ostensible authority, reinforced by estoppel principles, forecloses this defence[41].

VI. THE CONTRACTUAL DIMENSION: INDEMNITY CLAUSES & THEIR LIMITATIONS

A. Typical Bank–Vendor Contractual Arrangements

Banks and V-KYC providers usually enter into outsourcing agreements that are regulated by technology outsourcing contracts or master service agreements (MSAs)[42]. These contracts aim to distribute financial responsibility and operational risk resulting from V-CIP process failures.

The following are examples of common clauses:

1. Compliance Warranties: Suppliers specifically guarantee that their systems and practices adhere to the RBI Master Direction on KYC and all applicable data security laws.
2. Limitation of Liability Clauses: Vendors usually cap their total liability at the aggregate value of service fees or a pre-specified monetary limit (e.g., ₹10–50 lakhs), regardless of the actual loss caused1[43].
3. Indemnity Clauses: Vendors agree to indemnify and hold harmless the bank for any direct losses caused by their negligence, system failures, or confidentiality breaches.
4. Arbitration and Governing Law: Under the 1996 Arbitration and Conciliation Act, disputes between banks and suppliers are frequently submitted to private arbitration, which is exempt from civil court jurisdiction[44].

---

[39] Arjya B. Majumdar, *Vicarious Liability of Banks for Outsourced Operations: A Comparative Study*, 8 J. INT'L BANKING L. & REG. 445 (2019).
[40] District Coop. Bank Ltd. v. Leelawati Devi, 2020 SCC OnLine NCDRC 1057.
[41] Renuka Sane & Ajay Shah, *The Evolution of Consumer Protection Regulation in Indian Finance*, 3 J. FIN. REG. 67 (2017).
[42] Reserve Bank of India, Master Direction – Know Your Customer (KYC), 2025, ¶ 23.4.
[43] Sample Bank–Vendor Agreement, Indemnity Clause (on file with author).
[44] Arbitration and Conciliation Act, No. 26 of 1996, § 7.

"The Vendor shall indemnify and hold harmless the Bank from any claims, losses, or damages arising out of or in connection with any failure or defect in the Video-KYC process, including but not limited to failures in liveness detection, data verification, or identity matching," states a standard indemnity clause[45].

Although this provision seems protective, it is solely contractual in nature and only regulates the bank-vendor relationship. It does not give consumers, fraud victims, or other financial institutions hurt by the KYC failure any immediate rights or remedies. Therefore, these clauses serve as mechanisms for intra-corporate risk distribution rather than as tools for consumer protection[46].

B. Why Indemnity Clauses Do Not Protect Consumers

1. Privity of Contract

Only parties to a contract may enforce its terms or take use of its advantages, according to the doctrine of privity. Banks and their vendors have a private contractual right to indemnity that is only available to them. No contractual relationship exists between the seller and a fraudulent third party, such as a client whose identity was stolen or a correspondent bank that loses money because of a mule account[47]. These third parties are unable to bring a direct lawsuit against the vendor for carelessness or violation of a legal obligation. Their sole option is to sue the bank, which will then have to pursue indemnity from the vendor in a different contractual action. Deterrence against KYC compliance breaches is weakened by this two-step enforcement framework, which also makes recovery more difficult and disperses culpability[48].

2. Practical Limitations

There are substantial practical obstacles to recovery even in cases where a bank properly asserts its indemnification. Many of the V-KYC vendors are small, venture-backed digital businesses that lack a strong balance sheet and capitalization. Liability limitations are a common feature of indemnity clauses, which limit compensation to a portion of the overall harm, usually equal to a few months' worth of service fees[49].

Furthermore, it is becoming more challenging to demonstrate vendor negligence in AI-based verification systems because algorithmic conclusions are opaque and difficult to verify ("black box problem"). Banks have to prove that the fraud was the product of the vendor's error rather than of clever criminal evasion; this is made more difficult by proprietary AI systems.

---

[45] *Id.*, Limitation of Liability Clause.
[46] Id. ¶ 12.3.
[47] Reserve Bank of India, Discussion Paper on Digital Lending: Guidelines for Balance Sheet Lenders and Service Providers, 2022.
[48] RBI Master Direction on Outsourcing of Financial Services by Banks, 2024, ¶ 8.2.
[49] OECD Report on Artificial Intelligence and Financial Consumer Protection (2023), at 44.

Last but not least, the two-stage litigation paradigm, in which clients sue the bank and the bank then sues the vendor, results in protracted delays in payment. This multi-step procedure erodes public confidence in digital KYC procedures and undercuts the deterrent effect of liability[50].

3. The Unfair Contract Terms Problem

An important new dimension to this conversation is brought about by the Consumer Protection Act of 2019[51]. According to Section 2(9), a contract is considered "unfair" if it materially alters the rights or duties of the consumer to the detriment of the customer[12]. Standard-form terms are used in many banks' customer agreements to try and limit the bank's responsibility for vendor failures. "The Bank shall not be liable for any errors, interruptions, or failures in services provided by third-party vendors engaged for video-KYC"[52] is a common disclaimer.

It is quite doubtful whether such disclaimers can be enforced. In the case of *Central Inland Water Transport Corporation v. Brojo Nath Ganguly*[53], the Supreme Court ruled that standard-form (adhesion) contracts that contain unconscionable clauses are null and unenforceable due to public policy violations. Customers are powerless to negotiate or change such agreements, especially in banking transactions.

Furthermore, clients cannot effectively "opt out" of KYC because it is a regulation requirement for using any banking service. A disclaimer that transfers the risk of vendor failure to the client essentially nullifies a legislative obligation and violates public policy. Such provisions would probably be considered unfair and unenforceable under the Consumer Protection Act.

Therefore, the non-delegable statutory responsibility imposed by Section 35A of the Banking Regulation Act[54] and Section 12[55] of the PMLA cannot be overridden by contractual attempts by banks to disclaim culpability for the faults of their contractors. Indemnity clauses do not negate customers' legal authority to hold banks responsible for KYC errors, even if they divide risk internally between banks and vendors.

[50] Sample Terms and Conditions, HDFC Bank Video-KYC Service (2025), Clause 14.
[51] Consumer Protection Act, No. 35 of 2019, § 2(9).
[52] *Id.*, Clause 16.
[53] Central Inland Water Transport Corp. v. Brojo Nath Ganguly (1986) 3 SCC 156.
[54] Banking Regulation Act, No. 10 of 1949, § 35A, (1949).
[55] Prevention of Money Laundering Act, No. 15 of 2003, § 12,(2003).

VII. THE DEEPFAKE MULE ACCOUNT DOCTRINAL ILLUSTRATION: LIABILITY IN ACTION

A. Facts

In 2024–2025, India saw a record-breaking surge in the creation of mule accounts connected to money-laundering and cyber-fraud. More than 450,000 mule accounts were frozen nationwide, according to data released by the Indian Cybercrime Coordination Centre (I4C). Of these, about 40,000 were in SBI and 10,000 were in Punjab National Bank, with additional clusters in Canara Bank, Kotak Mahindra Bank, and Airtel Payments Bank[56]. The RBI made it possible for these accounts to be opened through V-KYC procedures under its Master Direction on KYC, 2023, and the updated Master Direction on KYC, 2025.

AI-generated deepfake videos were exploited by an organized criminal network to pose as real people and submit forged identity documents during the V-KYC onboarding process in a particularly well-known event known as the *Deepfake Mule Account Case*[57]. A licensed V-KYC vendor, known as "Vendor X," was used by the network, which operated in several states, and was classified as a *"authorised service provider"* in accordance with RBI regulations. Both Vendor X's facial recognition and liveness detection systems were unable to identify the fakes. These fictitious identities were used to successfully open about 847 accounts across six institutions in a three-week period.

More than 200 victims were duped by these accounts, which laundered close to ₹50 crore in criminal assets. Many of these victims had invested in phony cryptocurrency and investment programs that were advertised using deepfake videos that purported to be RBI Governor Shaktikanta Das[3]. The Ministry of Home Affairs' Cybercrime Division ordered banks to freeze the accounts and opened criminal investigations after receiving complaints.

B. Legal Questions Arising

Under India's Banking and Financial crime structure, the episode poses urgent issues about civil and regulatory culpability. When mule accounts receive overseas remittances and domestic banks neglect to check customer names, correspondent banks frequently suffer losses due to fraudulent charge-backs. For regulatory violations or carelessness in KYC due diligence, may Bank Y (the primary responder bank) be held accountable to these correspondent institutions?

1. Obligation to Victims of Cyberfraud: Even if the fraud was carried out using an outsourced vendor's V-KYC process, do the investors and end users whose money was laundered through these accounts have a right to compensation directly from Bank Y?

[56] Press Release, Indian Cybercrime Coordination Centre (I4C), Illegal Payment Gateways Created Using Mule/Rented Accounts (Oct. 28, 2024).
[57] Deccan Herald, Cybercrime Surge: Over 65,000 Mule Accounts Detected in Karnataka in 2024 (June 12, 2024).

2. Liability of Real Identity Holders: Under section 12 of the PMLA[58] and section 35A of the Banking Regulation Act, 1949[59], are real identity holders entitled to damages for negligence or breach of statutory duty in cases where criminals use stolen Aadhar credentials or PAN numbers.
3. A Bank Y's defensive arguments would probably include the following: (a) Vendor X was an RBI "approved vendor"; (b) the bank had an indemnity clause in its outsourcing contract that protected it from vendor negligence; and (c) the bank had performed due diligence before hiring the vendor and had regularly audited compliance.
This essay contends that these defences do not, however, release one from vicarious or statutory liability.

C. Application of the Vicarious-Liability Framework

1. Non-Delegable Statutory Duty

It is a non-delegable obligation under PMLA § 12 that *"every banking company shall verify the identity of its clients and maintain records of transactions."* In a similar vein, RBI is authorised by § 35A of the Banking Regulation Act to issue legally binding directives that directly require compliance from the regulated business[60]. Administrative convenience may be achieved by outsourcing V-KYC operations, but the statutory burden will not be met. Contracting out operational responsibilities cannot abandon statutory duties, according to the *J.Y. Kondala Rao v. Andhra Pradesh State Road Transp. Corp.,* concept. Therefore, Bank Y is still accountable even if Vendor X fails[61].

2. Agency and Ostensible Authority

In Bank Y's name and on its behalf, Vendor X carried out the KYC verification. Through the bank's official online portal, customers engaged with Vendor X, who they perceived as acting as their representative. A principal who appoints another as its agent cannot thereafter deny liability, according to the idea of apparent authority. This is supported by the logic of Ocean Frost [1986] AC 717, which states that an entity cannot deny agency when faced with accountability while claiming independence when it suits them[62].

3. Public Policy and Loss Distribution

Considerations of public policy also support vicarious responsibility. Through contractual leverage, banks are better able to regulate vendor standards, insure against losses, and internalize compliance risk. Deciphering intricate outsourcing chains and pursuing tiny

[58] Prevention of Money Laundering Act, 2002, § 12.
[59] Banking Regulation Act, 1949, § 35A.
[60] Prevention of Money Laundering Act, 2002, § 12.
[61] J.Y. Kondala Rao v. Andhra Pradesh State Road Transp. Corp. (1961) 1 SCR 642.
[62] The Ocean Frost [1986] A.C. 717 (H.L.) (UK).

technology vendors are impractical tasks for victims of identity-based or deepfake frauds. Entities that possess regulatory privileges are required to assume the associated systemic risk, as was noted in *State Bank of India v. Shyama Devi*[63]. Bank Y should therefore be deemed vicariously accountable to reimburse the victims and the banks that were contacted.

4. Failure of Defences

Bank Y's dependence on Vendor X's "authorised" status is ineffective since regulatory approval results in a transfer of liability. Given the principle of privity of contract, the indemnification clause safeguards the bank internally but cannot eliminate the rights of third parties. Furthermore, the bank's assertion of "due diligence" does not absolve it of its statutory obligation; compliance responsibility is still non-delegable.

VIII. PROPOSED LEGAL FRAMEWORK: RESOLVING THE PARADOX

A. Interpretation of Existing Law: Why Banks Should Be Held Vicariously Liable

1. Statutory Duty Under the PMLA is Non-Delegable

India's financial integrity system is based on the PMLA. According to Section 12(1)[64], "every banking company, financial institution, or intermediary shall maintain records, verify, and furnish information relating to transactions". As such, the obligation is non-transferable, positive, and personal. It affixes to the "banking company" itself, not to any vendor, consultant, or contractor.

No clause in the PMLA permits the assignment of this responsibility to outside parties. Thus, any outsourcing of the V-CIP in accordance with the RBI Master Direction on KYC, 2025, is only an administrative delegate and does not constitute a transfer of legal responsibility.

Indian courts have continuously maintained that statutory obligations cannot be delegated. In the case of *J.Y. Kondala Rao v. Andhra Pradesh State Road Transp. Corp.*[65], it was decided that private agreements could not be used to circumvent legislative duties imposed in the public interest. Similarly, the Supreme Court reiterated in *M.C. Mehta v. Union of India*[66] that, independent of any outsourcing arrangement, entities tasked with public safety or compliance requirements must personally supervise adherence.

Therefore, even though RBI regulations may allow the use of "authorised vendors" for digital verification, the bank retains ultimate liability under Section 12 of the PMLA[67] and Section

[63] State Bank of India v. Shyama Devi (1978) 3 SCC 399.
[64] Prevention of Money Laundering Act, 2002, §12(1).
[65] J.Y. Kondala Rao v. Andhra Pradesh State Road Transp. Corp. (1961) 1 SCR 642.
[66] M.C. Mehta v. Union of India (1987) 1 SCC 395.
[67] M.C. Mehta v. Union of India (1987) 1 SCC 395.

35A of the Banking Regulation Act, 1949[68]. Although delegation can increase efficiency, legal accountability, a norm firmly established in administrative jurisprudence- is not diminished.

2. Ostensible Authority Doctrine

Banks are vicariously liable under agency principles, even in the absence of legislative duty. A principal who permits someone else to operate as its agent and a third party legitimately relies on that representation is obligated to abide by the agent's actions, according to the theory of apparent authority[69].

Customers only engage with the bank via its digital interface when using V-KYC. As a component of the bank's ecosystem, the vendor shows up on-screen, frequently displaying the bank's name, logo, or channel of contact. This sense of legitimacy and authority is further reinforced by the RBI's use of the term "authorised vendor."

According to the ruling in *Freeman & Lockyer v. Buckhurst Park Properties (Mangal) Ltd.*[70], which was later upheld in India by *Syed Abdul Khader v. Rami Reddy*[71], a principal cannot later deny actions taken by an apparent agent, particularly when the claim caused reliance. Customers upload private papers here because they think the verifier is the bank; as a result, the bank is legally responsible for any fraud or failure in the verification process.

Furthermore, the *Ocean Frost*[72] concept makes it clear that a principal cannot *"dispel control when liability arises and assert independence when convenient."* When sellers are designated as *"authorised"* by the RBI, it suggests approval and authority[73]. Therefore, rather than being a simple independent contractor, the vendor acts as the bank's agent in law and equity.

V-KYC is a fundamental component of statutory compliance and not a supplementary administrative activity when viewed through the lens of regulatory policy. Without maintaining responsibility, outsourcing such a crucial task compromises the KYC regime's overall integrity. Accordingly, banks are held vicariously liable for vendor breaches under both agency law and statutory interpretation.

3. Policy Rationale: Loss Distribution and Regulatory Justice

Economic fairness and logic are reflected in vicarious liability, which is more than just a punitive theory. Banks gain a lot from outsourcing, including lower onboarding expenses, quicker processing, and expandable online access. They are forced to absorb the risk that comes with these financial benefits.

---

[68] Banking Regulation Act, 1949, §35A.
[69] Pollock & Mulla, LAW OF AGENCY AND PARTNERSHIP IN INDIA (2020 ed.).
[70] Freeman & Lockyer v. Buckhurst Park Properties (Mangal) Ltd. [1963] 2 QB 480.
[71] Syed Abdul Khader v. Rami Reddy (1979) 2 SCC 601.
[72] The Ocean Frost, [1985] 1 Lloyd's Rep 1 (HL).
[73] RBI, Master Direction – Know Your Customer (KYC) Directions, 2025 (Draft).

According to the loss-distribution principle, which was stated by Calabresi and Posner in the law-and-economics literature[74], the party with the best ability to track performance, prevent injury, and effectively distribute losses should be held liable. Customers lack the insurance capacity, compliance teams, and resources that banks have to reduce risk. Additionally, banks have access to regulatory benefits that suppliers do not, such as RBI license and deposit insurance. Privilege brings duty. It would be unfair and discouraging to let banks externalize KYC risk while enjoying the advantages of regulatory license.

The logic aligns with the idea of *State Bank of India v. Shyama Devi*[75], which states that financial organizations who choose to use intermediaries or create intricate systems must likewise suffer the repercussions of their actions. Therefore, holding banks accountable satisfies the requirements of consumer protection, economic viability, and legal responsibility.

B. Proposed Statutory Amendment: Joint and Several Liability

To address the ambiguity between operational outsourcing and regulatory accountability, a specific liability clause should be added to the *RBI Master Direction on KYC, 2025*:

Clause X: Liability for Outsourced V-KYC

(1) If a regulated entity contracts with an authorised vendor to handle the V-CIP, both the regulated entity and the vendor will be held jointly and severally responsible for any losses or damages incurred by a customer or third party as a result of the V-KYC process's failure.

(2) Nothing in the vendor-regulated entity agreement will restrict the regulated entity's obligation to clients or other parties.

(3) The vendor may provide the regulated entity with indemnity in accordance with the terms of the contract, but this will not lessen its duty under subclause (1).

(4) The term *"failure of the V-KYC process"* encompasses, but is not restricted to, the following: (a)Inadequate or inaccurate identity confirmations; (b)Not spotting document forgeries, impersonation, or fake identities; (c) The establishment of an account without authorization due to technical or operational errors.

Justification: *Per Section 79(3) of the Information Technology Act of 2000 and Section 26 of the Securities and Exchange Board of India Act of 1992, this provision is similar to the joint and several liability concept*[76]*. Outsourcing in neither framework releases regulated companies from fundamental responsibilities. In addition to guaranteeing regulatory responsibility and protecting consumers, the amendment permits banks to pursue private indemnity claims against careless contractors.*

[74] Calabresi, The Costs of Accidents (1970); Posner, Economic Analysis of Law (1986).
[75] State Bank of India v. Shyama Devi (1978) 3 SCC 399.
[76] Information Technology Act, 2000, §79(3); *See also* SEBI Act, 1992, §26.

By codifying this responsibility sharing, the RBI would close the interpretive vacuum that currently impedes the enforcement of digital compliance by giving banks, fintech providers, regulators, and customers statutory certainty.

C. Complementary Measures

1. Mandatory Insurance

To close the interpretive gap that now impedes the enforcement of digital compliance, the RBI would formalize this liability sharing and give statutory clarity to all parties involved, including banks, fintech vendors, regulators, and consumers.

2. Vendor Certification and Audit

A vendor certification system like to the CERT-In accreditation in cybersecurity regulation ought to be established by the RBI. Vendors would be subject to yearly third-party audits that evaluate (a) algorithmic accuracy rates, (b) the effectiveness of fraud detection, and (c) compliance with data privacy laws[77]. Transparency should be improved by making the results publicly available. The *"authorised"* status must be revoked or suspended for persistently poor performance. As opposed to merely being a contractual designation, this guarantees that "authorization" represents actual compliance capacity.

3. Consumer Compensation Fund

The SEBI (Stock Brokers) Regulations, 1992's Investor Protection Fund and the Deposit Insurance and Credit Guarantee Corporation (DICGC) framework should serve as the models for the establishment of an industry-funded V-KYC Compensation Fund. To finance the fund, a small fee, such as 0.1% of each V-KYC transaction fee, could be used[78]. Victims should get temporary compensation within 30 days while the bank and vendor settle their liability separately. The public's confidence in digital onboarding systems is maintained and prompt consumer redress is guaranteed.

D. Synthesis: Towards a Coherent Liability Architecture

The aforementioned changes create a three-tiered ecosystem for accountability: (a) Primary liability: Under statutes and agency principles, banks continue to be directly liable to regulators and consumers. (b) Secondary recourse: In the event of operational negligence, banks may pursue insurance recovery or indemnity from suppliers. (c) Tertiary safeguard: The Compensation Fund and required vendor insurance provide victims with security.

By balancing efficiency and equity, these steps establish a digital compliance framework that is in accordance with global best practices for outsourcing in the financial industry (e.g., EU, 2019 EBA

[77] CERT-In, Empanelment Guidelines for Cybersecurity Auditors, 2020.
[78] IRDAI, Guidelines on Professional Indemnity Insurance for Intermediaries, 2021.

Guidelines on Outsourcing; Basel Committee's Principles on Outsourcing, 2023)[79]. By explicitly defining culpability, the suggested approach removes any room for interpretation, boosts customer trust, and pushes banks and vendors to absorb the risks associated with their technology decisions. This turns *"authorization"* into true accountable oversight.

IX. CONCLUSION

With the rapid digitization of banking in the form of the V-KYC system, financial inclusion has been revolutionized, but it has also highlighted a large ethical and legal loophole in India's regulatory system. The "Deepfake Mule Account" fiasco is a warning that the public trust in the financial system can be impaired by technological developments ahead of legislative developments. The unclear responsibility brought about by technology malfunctioning is the actual issue, not the use of AI itself. Banks have a non-delegable legal duty to verify the identity of their clients under the Banking Regulation Act of 1949 and the PMLA of 2002. Outsourcing contracts or indemnity conditions with suppliers cannot dilute this duty. The RBI's 2025 Master Direction has blurred the distinction between legal responsibility and operational delegation by creating the concept of "authorised vendors". The law of non-delegable duty, ostensible authority, and vicarious liability notwithstanding, it becomes clearly obvious that the responsibility lies with the banks. The organization enjoying legality, trust, and confidence of the public is finally answerable for preserving the integrity of the verification process, although vendors might execute it.

Relying on vendor independence to escape culpability would deprive misled customers, correspondent banks, and investors of an effective remedy, destabilizing the system and financial justice. Due to this, courts should apply the V-KYC framework by the mandates of fair risk distribution, deterrent, and consumer protection. In essence, as India moves toward the age of AI-based banking, it must reaffirm that legal culpability cannot be sacrificed at the altar of technical convenience. To ensure that these digital innovations remain rooted in the eternal notion that the duty to comprehend and protect one's customers cannot be outsourced, the legislation has to adapt rapidly.

[79] Basel Committee on Banking Supervision, Principles for the Sound Management of Third-Party Risk, 2023.