# NATIONAL LAW UNIVERSITY, JODHPUR

# SCHOLASTICUS

VOLUME XII, ISSUE I | MARCH, 2025 | ISSN: 0975-1157


## ARTICLES


- **Tariffs, Funds, and Financial Sovereignty: Reassessing the Gift City Paradigm in Light of IFSA's 2025 Regulatory Framework**
  *Utkarsh Vijayvargiya & Krishna Dabhi*

- **Code, Credit, and Control: Recalibrating RBI's Digital Lending Directions, 2025 between Innovation and Accountability**
  *Nupur*

- **Vicarious Liability for V-KYC failures: Resolving the "Authorised Vendor" Paradox under India's Digital Banking Framework**
  *Jahnavi Choubey & Anushka Sharma*

- **Central Bank Digital Currencies & Cross-border Payments: India's Digital Rupee Experiment in a Fragmented Global Financial Order**
  *Shivalik Pal & Mahak Khirwal*

- **The DPDA Act and Kerala Bank: a Case Study in Data Governance and Risk Management**
  *Adv K Gopika & Adv K Devika*

- **Recalibrating Blended Finance: The Indian Regulatory Framework and the IFSCA Shift**
  *Nimish Maheshwari & Aditya Baheti*


## EDITORIAL


- **Banking on Data, Betting on Trust: The Privacy Reckoning of India's Financial Sector.**
  *Anshita Rani*

SCHOLASTICUS

Volume XII, Issue I MARCH, 2025

**Patron**

Prof. Dr. Harpreet Kaur

*Vice-Chancellor, National Law University, Jodhpur*

**Editor-in-Chief & Faculty Coordinator**

Dr. Anand Kumar Singh

*Assistant Professor, National Law University, Jodhpur*

**Student Editorial Board**

Anandita Srivastava
*Student Chief-Editor*

Anshuman Srivastava
*Student Chief-Editor*

Pravit Vir Sarmah
*Managing Editor*

**Senior Associate Editors**

Aditya Karol

Anshita Rani

Soumya Agarwal

**Technical Editor**

Prince Ranjan

**Associate Editors**

Arav Tiwari

**Copy Editors**

Prince Ranjan

Vansh Garg

Chaitanya Mawalia

Mahak Taparia

**Published by**

The Registrar, National Law University, Jodhpur

ISSN: 0975-1157 | Centre for Studies in Banking and Finance,

National Law University, Jodhpur

## TABLE OF CONTENT

TARIFFS, FUNDS, AND FINANCIAL SOVEREIGNTY: REASSESSING THE GIFT CITY PARADIGM IN LIGHT OF IFSCA'S 2025 REGULATORY FRAMEWORK..... 1
*Utkarsh Vijayvargiya & Krishna Dabhi*
CODE, CREDIT, AND CONTROL: RECALIBRATING RBI'S DIGITAL LENDING DIRECTIONS, 2025 BETWEEN INNOVATION AND ACCOUNTABILITY ..... 25
*Nupur*
VICARIOUS LIABILITY FOR V-KYC FAILURES: RESOLVING THE "AUTHORISED VENDOR" PARADOX UNDER INDIA'S DIGITAL BANKING FRAMEWORK..... 40
*Jahnavi Choubey & Anushka Sharma*
CENTRAL BANK DIGITAL CURRENCIES & CROSS-BORDER PAYMENTS: INDIA'S DIGITAL RUPEE EXPERIMENT IN A FRAGMENTED GLOBAL FINANCIAL ORDER ..... 61
*Shivalik Pal & Mahak Khirwal*
THE DPDP ACT AND KERALA BANK: A CASE STUDY IN DATA GOVERNANCE AND RISK MANAGEMENT..... 82
*Adv K Gopika, & Adv K Devika*
RECALIBRATING BLENDED FINANCE: THE INDIAN REGULATORY FRAMEWORK AND THE IFSCA SHIFT ..... 103
*Nimish Maheshwari & Aditya Baheti*
BANKING ON DATA, BETTING ON TRUST: THE PRIVACY RECKONING OF INDIA'S FINANCIAL SECTOR..... 116
*Anshita Rani*

Utkarsh Vijayvargiya & Krishna Dabhi, *Tariffs, Funds, and Financial sovereignty: Reassessing the GIFT City Paradigm in Light of IFSCA's 2025 Regulatory Framework,* 12 (1) SCHOLASTICUS 1 (2025).

# TARIFFS, FUNDS, AND FINANCIAL SOVEREIGNTY: REASSESSING THE GIFT CITY PARADIGM IN LIGHT OF IFSCA'S 2025 REGULATORY FRAMEWORK

*Utkarsh Vijayvargiya[*] & Krishna Dabhi[†]*

*ABSTRACT*

*India's GIFT City – the nation's only International Financial Services Centre (IFSC) has become an increasing destination for cross-border fund management within the collective regulatory jurisdiction of the International Financial Services Centres Authority (IFSCA). This is while a reignited US–China tariff war 2024–25 has shaken global trade, leading investors and fund managers to search for alternative markets. This article revisits the GIFT City model against these dynamics, particularly the new IFSCA (Fund Management) Regulations, 2025. We map the development and legal framework of GIFT City, examine the 2025 Fund Management Regulations, and evaluate global spillovers from US trade policy. We borrow comparative lessons from traditional fund jurisdictions (Singapore, DIFC, ADGM, Luxembourg) and survey the significant enforcement precedents (e.g., Sahara India). The interaction between shield tariffs and fiscal relocation delivers challenges and opportunities: India's comparatively home-based economy can ride out trade shocks (IMF/World Bank reports) and even pull in capital displaced from China (Reuters, 2025; East Asia Forum, 2025). Still, GIFT City must fill gaps in regulation, taxes, and operations to take advantage of this window. We end with policy advice to support GIFT's competitiveness and harmonise its fund regime with international best practice. This authoritative, law-and-policy analysis demonstrates that although GIFT City has progressed (177 FMEs), US$22.1 bn commitments up to mid-2025Further reforms are required to cement its role as a regional fund-management centre in the face of increased geopolitical risk. Further reforms are required to cement its role as a regional fund-management centre in the face of increased geopolitical risk.*

[*] Utkarsh Vijayvargiya is a second year B.B.A. LL.B. student, at Indian Institute of Management, Rohtak, and can be contacted at vijayutkarsh7[at]gmail[dot]com

[†] Krishna Dabhi is a Second year B.B.A. LL.B. student, at Indian Institute of Management, Rohtak, and can be contacted at krishnaiimr04[at]gmail[dot]com

## I. INTRODUCTION

The Indian government has established GIFT City (Gujarat International Finance Tec-City) to facilitate an offshore financial platform within India's framework. The IFSCA was established as a unified regulator for all financial service activities in India's IFSCs, through the International Financial Services Centres Authority Act, 2019. The GIFT City IFSC offers a "best-in-class regulatory framework" and tax regime under which Indian and global institutions can offer cross-border financial services.[1] Prime Minister Modi set the goal of establishing GIFT City as "a price-setter for … financial instruments", combining India's onshore with an offshore regulatory environment. In the first three years since its 2020 launch, GIFT's fund-management ecosystem has rapidly grown. Projections through the end of 2024 show 139 Fund Management Entities (FMEs) operating 198 funds with commitments of US$14.88 billion. Its growth has been led by progressive regulation and tax incentives. For example, and as noted above, by its regulatory reforms (2022–25), the IFSCA aligns itself with global regulations related to stipulations, while India's Income Tax Act provides an overseas taxation neutral regime for offshore funds reallocated to GIFT City.[2]

At the same time, the world is facing a new round of trade protectionism. In 2024–25, the US re-escalated tariffs on Chinese products over 125%, which prompted retaliatory actions and increased economic uncertainty. According to the WTO and IMF, this uncertainty appears to reduce global trade, 2025 forecasts updated to <1% growth due to tariffs impacting investment and supply chains.[3] Emerging Asia sees uneven spillovers; some economies tightly connected to China may see capital outflows, while others such as Vietnam and Malaysia wish to attract the capital that no longer goes to China.[4] So far, global investors have pulled over US$12 billion out of China-focused equity funds in early 2025. In this context, Asian financial centres are preparing to benefit.

---

[1] International Financial Services Centres Authority (IFSCA), *Fund Management ecosystem at GIFT-IFSC records robust growth amid IFSCA's progressive regulatory reforms* (Press Release, Aug. 7 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf. (ifsca.gov.in)

[2] Bijal Ajinkya & Rahul Jain, *Taxation of IFSC Funds and its Investors*, 37 Chamber's Int'l Tax J. (Sept. 2023), https://www.khaitanco.com/sites/default/files/2024-02/CTC%20Journal%20-%20Article%20on%20Taxation%20of%20IFSC%20Funds%20and%20its%20Investors.pdf.

[3] Sushma Ramachandran, *Resilience in Times of Uncertainty: How India Navigates Tariff Whirlwinds with FTAs, Domestic Push*, The Secretariat (Oct. 8 2025), https://thesecretariat.in/article/resilience-in-times-of-uncertainty-how-india-navigates-tariff-whirlwinds-with-ftas-domestic-push.

[4] East Asia Forum, *Asia Must Brace for the Impact and Opportunities of Trade Tensions* (30 Nov. 2024), https://eastasiaforum.org/2024/11/30/asia-must-brace-for-the-impact-and-opportunities-of-trade-tensions/#:~:text=Increased%20tariffs%20on%20Chinese%20imports,goods%20produced%20in%20third%20countries.

Singapore recently surpassed Hong Kong in the rankings as a global financial centre, benefiting from stable policies while tensions between the West and China increased.[5]

This paper explores the role of GIFT City's fund management framework in responding to global upheaval. We start by reviewing India's IFSC establishment and some of GIFT City's purposes. Then, we analyse the IFSCA (Fund Management) Regulations, 2025 from a legal perspective, including new scheme types, governing structures and eased requirements. Following this, we survey the international backdrop: how the trade war between the US and China has changed capital flows and the competition for financial centre status. We outline helpful comparisons from Singapore's MAS, Dubai's DFSA and ADGM regimes and Luxembourg fund framework. A specific case study on *Sahara India Real Estate Corp. Ltd. v. SEBI (2012)* will highlight some enforcement mechanisms around cross-border funds. Finally, we canvass implications for GIFT City's positioning and consider the areas for public policy (tax, regulation, facilitation) where it could take action to improve GIFT City's attractiveness as a fund management location. In all cases, we highlight the most recent data sources and legal references to provide certainty in this developing area.

## II. RESEARCH METHODOLOGY

This study utilises a doctrinal and comparative research methodology to investigate the development and consequences of the IFSCA (Fund Management) Regulations, 2025, concerning the GIFT City framework amidst global trade uncertainties. The study utilises a variety of primary sources, including regulations, circulars, government notifications, and policy statements from the International Financial Services Centres Authority (IFSCA), to gain insight into the regulatory, legislative and policy context. The study considers some secondary sources, including research papers, industry reports, news articles, and commentaries from experts that provide background and contextual information on fund management trends and regulations around the world. The study will undertake a comparative review approach of the evolving regulatory framework in India against best practices globally for the professional fund manager, investing, regulation, investor protection, and development of the broader market. Limitations include reliance on and use of publicly available information, and the factors that an evolving regulatory environment will influence the type and scope of a real-time analysis. This methodology seeks to evaluate, provide gap analysis and ideally desk recommendations for the developing a fund management industry in GIFT City.

[5] GWBMA, *Singapore Overtakes Hong Kong to Become Asia's Top Financial Center*, Registration China (May 31, 2024), https://www.registrationchina.com/articles/singapore-overtakes-hong-kong-to-become-asias-top-financial-center/.

## III. EVOLUTION OF GIFT CITY AND INDIA'S IFSC FRAMEWORK

The idea of an Indian IFSC was first conceptualised in 2007, but picked up speed in the mid-2010s. The Government formally approved GIFT City as a Multi-Services Special Economic Zone under the SEZ Act of 2005 by notification in 2015–16. The International Financial Services Centres Authority Act, 2019 (No. 50 of 2019) statutorily established IFSCA as a single regulator for financial services in the IFSCs. Statement of Objects of the Act authorises IFSCA explicitly to "develop and regulate financial products, financial services, and financial institutions" in IFSCs.[6] Operationalised with effect from September 2020, IFSCA replaced RBI, SEBI, IRDAI, and PFRDA in regulating IFSCs, creating an integrated framework. This legislative integration was aimed at simplifying licensing and eliminating duplication. According to one commentator, IFSCA "replaced RBI, SEBI, etc. as the single point of regulation" within IFSCs.[7]

In the IFSC regime, the units are considered non-residents of India's exchange control and can transact in foreign currency. The tax policy is also customised; India provides special tax treatment to GIFT funds. Category I and II Alternative Investment Funds (AIFs) registered with SEBI already have pass through treatment for domestic investors. GIFT's Income Tax Act ensures neutrality for offshore funds shifting to the IFSC. A special domestic provision (Sec. 10(23FBC) of the Income Tax Act) guarantees that the investors in a Category III AIF (with non-resident investors only) set up at the IFSC don't pay any tax on their share of the income.[8] Investors are taxed 10% (the GIFT tax rate) at best, and there's no corporate minimum alternate tax. These incentives – coupled with capital gains and dividend distributions exemptions – seek to make GIFT IFSC competitive with world fund flows.

GIFT City was contemplated as a cutting-edge smart city and financial centre. India's "first fully functional smart city and the country's one and only IFSC" provides a smooth platform for economic and IT services. The focus is "onshore talent with an offshore technological and regulatory framework," as conceptualised by PM Modi. The IFSC is specifically required to serve customers outside India in any currency besides INR. The aim has been to "provide international financial services offering cross-border financial products and services in a competitive tax environment".[9]

---

[6] International Financial Services Centres Authority, *The International Financial Services Centres Authority Act, 2019*, Act No. 50 of 2019, https://www.indiacode.nic.in/bitstream/123456789/14009/1/A2019_____50.pdf.

[7] Parth Ved, *Financial Entities in IFSC: A Primer*, Vinod Kothari Consultants (Nov. 25, 2022), https://vinodkothari.com/2022/11/financial-entities-in-ifsc-a-primer/.

[8] Parul Jain, Dhruv Sanghavi, Prakhar Dua, Radhika Parikh, Nandini Pathak, and Parul Jain, *Fund Formation: Attracting Global Investors — Global, Regulatory and Tax Environment Impacting India Focused Funds* (Nishith Desai Associates, Feb. 2024), https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Fund-Formation-Attracting-Global-Investors.pdf.

[9] Z/Yen Group, *Focus on GIFT City 2024*, Financial Centre Futures (Nov. 2024), https://www.longfinance.net/media/documents/Focus_On_GIFT_City_2024_v1.3.pdf.

Early development has been encouraging. As per data from IFSCA, GIFT-IFSC's fund management ecosystem increased gradually during the 2024–25 period. By Q4 FY 2024–25 (Dec 31, 2024), 139 FMEs ran 198 schemes, with aggregate commitments totaling US$14.88 billion and funds raised US$7.01 billion. By June 30, 2025, those numbers had risen to 177 FMEs, 272 schemes, US$22.11 billion commitments and US$10.5 billion in funds (+40.5% quarter-on-quarter). Particularly, ~85% of investments have been directed towards India, "supporting the 'onshore the offshore' mantra" and making GIFT City an entry point into Indian assets.[10] The investor base is international: more than 3,500 overseas and domestic institutional investors across 60+ jurisdictions have already invested through GIFT funds (Mutual Funds, VCs, PE, pension & sovereign wealth funds, etc.). Such numbers indicate strong momentum in GIFT's fund hub, supported by investor faith.[11]

Although the legal and physical infrastructure of GIFT City has developed a world-class international airport, stock exchange, bank branches, and regulatory environment, obstacles persist. The GIFT entities have to contend with well-established international fund domiciles. Uncertainties in Hong Kong and openness in Singapore during geopolitical strain have already restructured Asia's financial pecking order.[12] Under these circumstances, India's policymakers have worked to keep GIFT's structure evolving. The first IFSCA Fund Management Regulations, 2022 notified on April 2022), set the ground for onshore managers in the IFSC. Later versions most notably the 2025 Regulations codify the regime further. We now examine the current legal regime at length.

## IV. THE 2025 IFSCA (FUND MANAGEMENT) REGULATIONS: LEGAL ANALYSIS

### A. Overview

In February 2025, IFSCA issued notice of the IFSCA (Fund Management) Regulations, 2025. These supersede the 2022 Regulations and are based on industry comments. A press release states that the 2022 rules were "thoroughly reviewed in 2025 after considering the perspectives of market

[10] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, Press Release (Aug. 7, 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf.

[11] International Financial Services Centres Authority, *Statistics for Fund Management Activities in GIFT IFSC as on December 31, 2024*, https://ifsca.gov.in/Common/PreviewPdf?id=21626bde60601ef44a0ed02201817bb7&fileName=Statistics_for_Fund_Management_activities_in_GIFT_IFSC_as_on_December_31__2024_20250818_0549.pdf.

[12] GWBMA, *Singapore Overtakes Hong Kong to Become Asia's Top Financial Center*, Registration China (May 31, 2024), https://www.registrationchina.com/articles/singapore-overtakes-hong-kong-to-become-asias-top-financial-center/.

participants," while maintaining the foundational framework.[13] The fundamental principle remains: entities wishing to manage funds must register with IFSCA as a Fund Management Entity (FME), and each fund or scheme must be approved by IFSCA through a "Private Placement Memorandum" (PPM). Notably, the FME concept is akin to SEBI's Alternative Investment Fund (AIF) framework, but more efficient, one FME can launch multiple schemes without separate registration for each fund. As one legal expert explains, IFSCA's FME is equivalent to SEBI AIF, but the FME model does not use duplicative approvals.[14]

2025 Regulations extend the AIF-like scheme types. schemes are divided by investment strategy. Venture Capital Schemes (VC), Restricted Schemes (for qualified or accredited investors only), etc., are examples. General public retail schemes are usually not allowed (as in other IFSCs). One of the most significant enhancements in 2025 is alignment with the needs of investors and minimising friction. Reg. 10, a PPM's validity period has been extended from 6 to 12 months. The initial corpus requirement for new schemes has been reduced from USD 5 million to USD 3 million.[15]Facilitating managers in raising funds more easily. Transitional relief is granted to older PPMs (short extensions permitted). These changes are a reaction to calls from industry for more flexibility.

**B. Scheme enhancements and investor safeguards**

The Regulations also add new provisions to encourage innovation and investor protection. A significant one is the accredited investor formal framework: sophisticated investors for example, institutions, high net worth individuals, family offices are defined under a new investor class, making it easier to market to them. In the same vein, IFSCA has made available a special regime to enable Indian NRIs/OCIs to invest between 100% in IFSC funds, subject to conditions.[16] The 2025 regulations formalise this by clarifying that Non-Resident Indians (NRIs) can subscribe to scheme units after meeting specific KYC and tax requirements.

The regulations also clarify custody and asset eligibility norms. FMEs must ensure that an IFSC-based custodian or trustee holds fund assets. Fund assets can include securities, derivatives, and

---

[13] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, Press Release (Aug. 7, 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf.

[14] Ved, *supra* note 7.

[15] Legality Simplified, *IFSCA Fund Management Regulations, 2025*, (Apr. 9, 2025), https://www.legalitysimplified.com/ifsca-fund-management-regulations-2025/.

[16] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, Press Release (Aug. 7, 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf.

permitted foreign investments subject to IFSCA/SEBI collaboration, e.g., the IFSC FPI/NRI route for Indian securities[17]. These provisions aim to maintain par with SEBI's AIF norms while leveraging IFSC advantages (e.g., greater global asset access).

Most importantly, IFSCA has regulated governance and capital adequacy. According to the 2025 rules, an FME should possess a minimum net worth of USD 0.5 million for foreign entities, equivalent, or as specified for the type of scheme. Essential personnel directors, senior officers, fund managers should be fit and proper and possess the required certifications. FMEs are subject to regular oversight, such as portfolio composition disclosures, risk management requirements, and material scheme changes (Reg. 19–31). Audited financials annually, and disclosures have to be submitted to IFSCA. These investor protection features are generally similar to those of other jurisdictions (e.g. MAS's LFMC guidelines and DFSA rules).

### C. Co-investments and special schemes

The 2025 Regulations and subsequent circulars allow for explicit co-investing through Special Purpose Vehicles (SPVs). IFSCA has introduced a framework whereby a venture or restricted scheme can establish one or more SPVs ("Special Schemes") to hold individual portfolio companies. This enables a manager to create a parallel fund vehicle to co-invest in a practical context besides the central fund. As the Lexology analysis indicates, SPVs can benefit from "protective segregation of liabilities" via a protected-cell structure.[18] Unlike some regimes, IFSCA allows for a single-asset SPV as long as it is a co-investment with another related company. This fits global trends; for example, ADGM's VCC and MAS's VCC allow for umbrella and segregated portfolio funds, respectively. The SPV mechanism provides more flexibility for private equity and VC managers.

### D. Third party fund management services

One of the significant developments is the formal approval for non-IFSC third party fund management. In July 2025, IFSCA amended the FM Regulations to permit FMEs to manage funds sponsored by a third-party manager. A foreign fund manager can "attach" with an IFSC-licensed FME to set up a fund under their FME license, with certain safeguards. This idea similar to outsourcing fund management is for funds that want to use IFSC infrastructure but want to

[17] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, Press Release (Aug. 7, 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf.

[18] Economic Laws Practice, *IFSCA Issues a Framework to Facilitate Co-investment by Venture Capital Schemes and Restricted Schemes*, Lexology (May 22, 2025), https://www.lexology.com/library/detail.aspx?g=842eeac6-13d0-4952-b9d8-7158fbae77f7&utm_.

leverage foreign expertise. According to the IFSCA circular July 2025, the Restricted Schemes must be for specified investments only and only for specific investors, and the FME is responsible to IFSCA. However, in contrast to the SEBI's AIF regime, SEBI does not explicitly permit third party managed funds under one license. This new approval could attract global managers looking to enter India.

**E. Comparison with SEBI AIF Framework**

While there are similarities between the scheme design under IFSCA and the SEBI AIF model, there are also some key differences. Most importantly, there is the concept of the FME itself. Under India's domestic SEBI regime, each AIF (fund) is a separate legal entity that registers separately. Under IFSCA, a single FME entity (per IFSCA license) can launch and manage multiple schemes under that license. As a result, when it comes to compliance, the manager tells IFSCA once and does not need compliance for each fund entity. On the other hand, the IFSC regime provides that FMEs have a minimum corpus and minimum investor requirements (e.g. 50 accredited investors for some schemes), which is very similar to SEBI's QIF/Expert AIF categories. IFSCA also mandates that all FMEs, even re-domiciled funds, maintain sufficient capital and otherwise meet prudential standards and definitions under the IFSCA Act. The 2025 Regulations overall seek to balance both India's desire to emulate global norms (e.g. co-investment SPVs, flexible structuring of investments) and investor protections, transparency, and disclosure (fit-proper checks, capital rules, and disclosure norms).

**F. key legal highlights**

1. PPM & Validity: Private Placement Memoranda (PPMs) of venture/restricted schemes are now valid for 12 months. IFSCA may, on request, extend expired PPMs by 6 months.[19]
2. Corpus: Scheme size is lowered to USD 3 million (earlier 5 million), promoting smaller funds.
3. Accredited Investor Framework: Institution and qualified investor formal definition and onboarding specifications have been added.
4. NRI/OCI Contribution: Relaxations have been made for a 100% NRI/OCI contribution to IFSC funds (via FPI route with safeguards).
5. Co-investment & SPVs: Special Schemes (SPVs) permitted co-investing VCs/restricted schemes.
6. Third-Party Management: FMEs allowed to manage funds on behalf of foreign/domestic third-party managers, subject to harsh conditions.[20]

[19] International Financial Services Centres Authority, *Transition to IFSCA (Fund Management) Regulations, 2025*, Circular F. No. IFSCA-IF-10PR/1/2023-Capital Markets/7 (Apr. 8, 2025), https://ifsca.gov.in/Document/Legal/transition-to-ifsca-fund-management-regulations-20250804202509312 1.pdf.

[20] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, Press Release (Aug. 7, 2025),

7. Transition Provisions: FMEs with schemes in operation by Feb 2025 are given grandfathering, including PPMs filed before the regulation date.

The 2025 Regulations reflect an incremental development of India's new regime for IFSC funds. They largely align GIFT City with high tier fund jurisdictions by introducing modern structures (e.g. co-invest SPVs, VCC draft), with regulatory robustness guaranteed. The reforms are critical to making GIFT City a competitive peer of Singapore, Dubai, or Luxembourg. We go on to the overall global context where these reforms will operate.

## V. THE GLOBAL BACKDROP: US TARIFF WAR AND FINANCIAL SPILLOVERS

Starting in 2024, US trade policy shifted unexpectedly and more aggressively. In addition to leaving tariffs on China above 100%, the US occasionally announced higher tariffs on the EU and other trading partners while temporarily retracting. Together, these tariffs have contributed to supply-chain uncertainty. The WTO reported revised global trade growth is now less than 1% as "tariff uncertainty weighed heavily on business confidence, investment and supply chains"[21] Empirical observers have noted that countries closely linked to China (ex., electronics exporters) may have immediate headwinds, whereas other countries will benefit by winning diverted production and investment[22].[23]

Financial markets responded sharply. A Reuters analysis cites that global investors are "more cautious on China" and have, in turn, recently withdrawn about US$12 billion from equity funds focused on Chinese exports. Fund managers report flight-to-safety flows, for example, into bonds or gold. In Asia, the January 2025 pullback in Chinese equities was partly attributed to a drawdown associated with tariffs.[24] Conversely, there have been times when sentiment toward other Asian markets has improved. Analysts cite Malaysia and Vietnam as receiving higher direct foreign investment as firms hedge their supply risk.[25].

---

https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf.

[21] Ramachandran, *supra* note 3.

[22] Takashi Onoda, *Asia Must Brace for the Impact and Opportunities of Trade Tensions*, *East Asia Forum* (Nov. 30, 2024), https://www.eastasiaforum.org/2024/11/30/asia-must-brace-for-the-impact-and-opportunities-of-trade-tensions/#:~:text=Increased%20tariffs%20on%20Chinese%20imports,goods%20produced%20in%20third%20countries.

[23] *Id.*

[24] Ankika Biswas, *Trade War or Not, Global Investors Turn Even More Cautious on China*, Reuters (Feb. 5, 2025), https://www.reuters.com/markets/asia/trade-war-or-not-global-investors-turn-even-more-cautious-china-2025-02-05/#:~:text=In%20the%20past%20three%20months%2C,October%27s%20inflow%20of%20%2413%20billion.

[25] Onoda, *supra* note 22.

There are also political aspects to consider. Increased tensions between the US and China influence Hong Kong's role. One observer noted that "geopolitical tensions ... build, Hong Kong, being part of China, has had its international status and attractiveness diminished," which has caused some institutions to relocate to Singapore.[26] Hong Kong's proximity to its competitors will favor Singapore's MAS-led environment (stable rule of law, open policy, etc.) and possibly other regional hubs that are not China. In fact, Singapore has recently changed its regulations (e.g., increasing retail access to private funds by long-term investment funds) to attract redirected global capital from riskier markets.[27].

Despite this, confidence is still fragile. A market commentator in April 2025 observed that any loosening of tariffs can "raise investor confidence across Asia, including in Hong Kong", but cautioned that "the trade-weighted effective tariff rate is still going up" and that some volatility is probably still forthcoming.[28]. In short, US protectionism provides both pressures and possibilities, and it is expected that Asia's next tier financial centres, which enjoy political stability and reliable regulation, may capture some of the flows being considered, +/- China.

GIFT City's implications are twofold. First, GIFT City should contribute to India's broader economic resilience to the trade war. Some commentators emphasise India's economy, accounting for only ~2% of world trade, to be relatively insulated. The domestic-focused nature of the Indian economy (GDP ~6-7%, mainly driven by consumption and services) provides some cushion. In fact, India is not seeing significant export growth, which tempers US tariffs significantly; India's services exports remain strong, and the nation is negotiating FTAs with the UAE and the UK, and looking to begin trade talks with the EU. Major agencies (ADB, IMF) still expect India to grow about ~6.5% in 2025, partly because the effects of the tariff war are "expected to be manageable as trade accounts for a relatively small share of GDP"[29]. GIFT City enjoys the benefit of the general resilience of a macro economy and international confidence in India's future.

Second, the tariff war provides market opportunities. If companies relocate supply chains out of China, some global companies may look to India for new assets (manufacturing, tech, etc.). Funds focused on Emerging Asia may even rebalance into Indian equities or local debt. GIFT City can

---

[26] *Singapore Overtakes Hong Kong to Become Asia's Top Financial Center*, Registration China (May 31, 2024), https://www.registrationchina.com/articles/singapore-overtakes-hong-kong-to-become-asias-top-financial-center/#:~:text=center%2C%20mainly%20due%20to%20Singapore%E2%80%99s,both%20Singapore%20and%20Hong%20Kong.

[27] Sidley Austin LLP, *Singapore Investment Management Regulatory Update (July 2025)*, Sidley Insights (July 3, 2025), https://www.sidley.com/en/insights/newsupdates/2025/07/singapore-investment-management-regulatory-update-july-2025#:~:text=In%20line%20with%20recent%20global,Singapore%20and%20authorized%20by%20MAS.

[28] Reuters, *Investors React to Intensifying Sino-US Trade Tensions*, Reuters (Apr. 10, 2025), https://www.reuters.com/markets/investors-react-intensifying-sino-us-trade-tensions-2025-04-10/#:~:text=,negotiation%20headlines%20take%20centre%20stage.

[29] Ramachandran, *supra* note 3.

serve as a hub for capital for such opportunities. According to one Indian report, a possible EU–India FTA (likely by 2025–26) could facilitate a substantial boost to exports and make India increasingly attractive to foreign investors. Hence, GIFT City and its fund regimes would be well-positioned to take advantage of this boost. However, it must contend with competition: investors worldwide can relocate their operations to Singapore or London or institutions elsewhere, like the Middle East (i.e., the ADGM or DIFC), with similar infrastructure. Within Asia, the selling points in GIFT City and IFSC are strong: a low tax rate of 10%, exposure to India's growth story, and a stable though developing legal system. However, these selling points must be assessed through the lens of perception; the IFSC is new and therefore not as tried and tested as Singapore or Luxembourg.

The US tariff war has unsettled agreeable business arrangements and caused capital re-evaluation. Global fund managers are more identified than ever to hedge future capital flows against a China-centric risk profile (as demonstrated by current fund flows)[30]. This is potentially positive for competing hubs. For GIFT City, this emphasises projecting confidence and competitive offerings. The coming sections look to consider how global jurisdictional practices and enforcement experiences impact where GIFT fits into this discussion.

## VI. COMPARATIVE LEGAL PERSPECTIVES: LESSONS FROM GLOBAL FINANCIAL HUBS

GIFT City will ultimately have to compete with existing international financial centres. We review fund-regime design in Singapore, Dubai (DIFC/DFSA), Abu Dhabi (ADGM), and Luxembourg to share applicable lessons. We will concentrate on structural and regulatory aspects that may be replicable or adaptable for India.

1. **Singapore (MAS):** Singapore's Monetary Authority of Singapore (MAS) has a long-standing approach to developing fund management for various investment funds. The regime separates fund managers into Licensed Fund Management Companies (LFMCs) and Venture Capital Fund Managers (VCFMs) based on capital/profit thresholds or restrictions for managing funds and disclosures. A hallmark of Singapore's regime is establishing a Variable Capital Company (VCC) structure, which was introduced in 2020 and permits open-ended umbrella funds with segregated sub-funds operating under a single corporate entity. The VCC resembles the FME/umbrella concept under IFSC. MAC has developed a complete package of tax incentives which is helpful for fund investors: the Singapore Resident Fund Scheme offers tax exemption for certain income, and funds can operate in Singapore as tax-exempt collective

[30] Biswas, *supra* note 24.

investment vehicles if more than 20% is qualified ownership by fund corporations. Recent MAS consultation/reform views proposed open access to the private market from retail investors, under MAS registered Long Term Investment Funds (LIFs), demonstrating a global trend toward democratized access to fund investment. Singapore's progression of easy licensing including fast-track applications for pre-approved funds and a stable political environment have resulted in thousands of funds from other centres in Singapore. The operating lessons for GIFT include the following: supported by good governance and a transparent process for licensing, Singapore encourages, facilitates, and rewards innovation (like the VCC structure and LIF concept) that broadens the appeal of investment vehicles[31].

2. **Dubai (DIFC-DFSA):** The Dubai International Financial Centre (DIFC), overseen by the DFSA, has an established multi-tier fund framework. This framework incorporates **Public Funds** (for mass retail and offers full disclosure), **Expert Funds** (with a maximum of 200 investors, no minimum AUM, marketed solely to qualified investors), and **Qualified Investor Funds** (QIFs) (a minimum of 50 investors and of $100,000); Qualified/Expert Funds have no minimum capital requirements. Notably, DIFC allows external (i.e., non-DIFC) fund managers to manage retail DIFC funds with no local licensing requirements from "acceptable jurisdictions". Additionally, DIFC grew in popularity with the Protected Cell Company (PCC) structure, which legally distinguishes sub-funds' assets within an umbrella fund. Fund custody and administration must be licensed at world-class levels of supervision. The cost to fund managers to establish a fund can be relatively low (e.g., USD 50K to develop a QIF). The DFSA takes a very pragmatic and commercial approach to regulation, emphasising touching the professional operator lightly while maintaining strong anti-money-laundering rules and allowing reputable global custodians from a significant international financial centre. For GIFT, it is worthwhile to consider DIFC's positive regulatory experience as providing value toward considering the implications of flexibility (e.g., DIFC has no domicile requirement for managers) and a legal segregation mechanism (e.g., PCC)[32]. GIFT's SPV regime is similar to the PCC concept of the DIFC
3. **Abu Dhabi (ADGM):** ADGM (Abu Dhabi Global Market) has been proactively courting fund managers, capitalising on factors described as "tax-friendly environment (0% corporate tax) and streamlined authorisation". Its Financial Services Regulatory Authority (FSRA) has

[31] Sidley Austin LLP, *Singapore Investment Management Regulatory Update (July 2025)*, Sidley Insights (July 3, 2025), https://www.sidley.com/en/insights/newsupdates/2025/07/singapore-investment-management-regulatory-update-july-2025.

[32] Dubai Financial Services Authority, *Funds in the DIFC* (Sept. 14, 2014), https://www.dfsa.ae/application/files/4815/8220/1483/FUNDS-in-the-DIFC-Sep-14-2014.pdf.

made funds available through companies, Limited Partnerships, or trusts. ADGM also launched its own VCC in 2021. It offers an innovative framework with a private REIT regime and a Venture Capital Fund Manager (VCFM) category with a zero capital requirement. There are no investor limits or AUM minimums for qualified funds, and there are no remuneration caps for managers. With proper approval, ADGM has an open approach: any entity (local or foreign) may market and distribute funds from ADGM. Their commitment to "best-in-class costs and time-to-market" aligns with UK Common Law, offering a welcome option for international fund managers. As ADGM provides a clean presentation of tax, an extensive range of fund vehicles (corporate, LP, trust), and a competitive fee structure, it has streamlined its services and processes. For example, ADGM takes pride in presenting no direct taxes, a wide selection of investment vehicles, and competitive fee structures to fund managers[33]. GIFT may leverage ADGM's playbook by ensuring transparent fees, ease of repatriating capital, and enforceable contracts in line with global best practice (for example, ADB offers to include ADGM arbitration clauses, etc.). Overall, the Middle Eastern model demonstrates that tax-neutrality combined with a clear legal framework (of 0% tax and the UK legal framework) has the potential to attract investment capital quickly

4. **Luxembourg (CSSF):** Luxembourg is unequivocally the largest fund domicile in Europe and provides a wide variety of fund structures, such as: Undertaking for Collective Investment in Transferable Securities ("UCITS" or regulated mutual funds), Part II funds, Specialised Investment Funds ("SIFs"), Reserved Alternative Investment Funds ("RAIFs") and partnership structures. RAIFs have become a very popular structure, as they are not regulated and only need to appoint an AIFM that is registered ("Alternative Investment Fund Manager"), which allows considerable flexibility while also providing European "passporting" under the AIFMD ("Alternative Investment Fund Managers Directive"). Luxembourg domiciled funds have access to broadly marketed funds throughout Europe, tax-passthrough arrangements often not taxable if the investor is taxed elsewhere, and very recent reforms demonstrating its competitiveness for instance tax at 2025 enabling broaden the carried interest regime, where carried remunerations continue to be lightly taxed, and also provides clear terms to be applied to the "reverse hybrid" tax rule in the collective-enforcement vehicle. Under the new legislation, it demonstrates that it wants to ensure that it continues to be one of the most attractive locations for private capital, also showing apparent regulatory and tax certainty in

[33] Abu Dhabi Global Market, *Investment Funds* (July 5, 2018), https://assets.adgm.com/download/assets/adgm-investment-funds.pdf/8a8dd708589b11ef9fab36e29b0f3a63.

these new reforms[34]. Key lessons: the regulatory framework and tax certainty are central. The GIFT City follows a similar exemption for the Framework as a draft amendment for the IFSC Act for being carried interest, to have comparable standards internationally. In Luxembourg, the requirement for funds to appoint AIFMs and auditors who are domiciled in the EU will ensure the funds adopt early on a level of rigor and trust with investors; however, GIFT allows either Indian managers or foreign managers who are licensed through the IFSCA. On balance, the European model of encouraging cross-border passporting (through agreements or mutual recognition between mainly countries) or tax-neutral fund vehicles that will attract fund managers.

A comparison brief is made in Table 1 below. Note how GIFT-IFSC (under IFSCA) has multiple similarities with the jurisdictions - a unified regulation, tax neutral, and choice of vehicles - but also several gaps (non-EU location, rulebook becoming current). Its competitive benefit comes from the large Indian market access and coherent policy push, and its weaknesses seem primarily from the brand not being recognised yet and aligning it with global practice (if introducing VCCs or umbrella funds from existing and creating what is more substantial).

**Table 1 – Fund Regime Comparison**

| **Feature/Regime** | **GIFT City (IFSCA)** | **Singapore (MAS)** | **Dubai DIFC (DFSA)** | **Abu Dhabi ADGM (FSRA)** | **Luxembourg (CSSF)** |
|---|---|---|---|---|---|
| **Regulator** | IFSCA (unified) | MAS | DFSA (DIFC) | FSRA (ADGM) | CSSF |
| **Fund Vehicle Types** | Fund Management Entity (FME) and multiple schemes; | LFMC + Variable Capital Companies (VCC) | Public Funds, Expert Funds, QIF (PCC) | VCC, Co. Ltd, LP, trusts; VCFM | UCITS; SIF; Part II UCI; AIF; RAIF |
| | segregated portfolio via SPVs | (umbrella open/closed) | (segregated cell umbrella) | (0% tax, umbrella allowed) | (umbrella and partnership funds) |

[34] Guilhèm Becvort, *Luxembourg's Push for Private Capital Attractiveness and Competitiveness*, White & Case (Sept. 9, 2025), https://www.whitecase.com/insight-alert/luxembourgs-push-private-capital-attractiveness-and-competitiveness.

| | | | | | |
|---|---|---|---|---|---|
| **Investor Types** | Accredited/Qualified; NRI/FPI eligible | Retail (LFMC target retail funds); | Qualified/Expert (only professional) | Accredited/investible | Retail (UCITS) & professional (AIF) |
| | | Accredited (private wealth) | | | |
| **Capital/Corpus Req'ts** | FME net worth USD 0.5M; Scheme min corpus USD 3M[35] | LFMC: SGD 1–2M capital; Funds often no AUM min[36] | QIF min USD 20k; Expert min 50 investors; no fixed AUM[37] | No fixed AUM; VCFM zero capital[38] | RAIF, SIF: no AUM; Part II: €1M; AIFMs: €125k–€300k capital |
| **Tax Regime** | GIFT tax: 10% on income; corporate tax 9%; fund income exempt | Offshore fund incentives: 0% for VCCs if conditions are met | 0% corporate tax; funds are generally tax-exempt | 0% corporate tax; 0% withholding | Funds are tax-transparent for EU investors |
| **Notable Features** | Onshore tax neutrality for foreign funds; co-invest SPVs; | Strong enforcement; VCCs allow sub-funds; | External managers can run DIFC funds without a | Business-friendly costs; 0% tax; flexible VC/REIT frameworks | EU passport via AIFMD; robust |

[35] Legality Simplified, *IFSCA (Fund Management) Regulations, 2025*, Legality Simplified (Apr. 9, 2025), https://www.legalitysimplified.com/ifsca-fund-management-regulations-2025/.
[36] Sidley Austin LLP, *Singapore Investment Management Regulatory Update (July 2025)*, Sidley Insights (July 3, 2025), https://www.sidley.com/en/insights/newsupdates/2025/07/singapore-investment-management-regulatory-update-july-2025#:~:text=In%20line%20with%20recent%20global,Singapore%20and%20authorized%20by%20MAS.
[37] Dubai Financial Services Authority, *Funds in the DIFC* (Sept. 14, 2014), https://www.dfsa.ae/application/files/4815/8220/1483/FUNDS-in-the-DIFC-Sep-14-2014.pdf.
[38] Abu Dhabi Global Market, *Investment Funds* (July 5, 2018), https://assets.adgm.com/download/assets/adgm-investment-funds.pdf/8a8dd708589b11ef9fab36e29b0f3a63.

| | | | | | |
|---|---|---|---|---|---|
| | third-party fund mgmt[39] | MAS LIF for retail[40] | local license[41]; PCC structure | | regulatory oversight; evolving carried-interest carve-outs[42] |

(*Sources: IFSCA Regulations, 2025; MAS/FSC publications; DFSA/ADGM brochures; White & Case (2025) on Luxembourg.*)

In reviewing comparative ways, GIFT City identified, asserted, and/or utilised many best practices (e.g., single unified regulator, tax neutrality, flexible SPVs). Like regulatory playbook standards, GIFT City's approach is converging with the rest of the world: e.g., draft proposals to execute a new Variable Capital Company (VCC) regulatory platform at the IFSC.[43] Largely parallels proposed changes in SG/ADGM. However, GIFT's relatively small scale means it would take time to reach the volume of funds domiciled in Singapore or Luxembourg. To enhance GIFT's position, it should continue benchmarking regulation, including emerging norms globally related to ESG disclosure and AML/KYC, and fund-of-funds indexing to enable funds to redirect capital efficiently based on investor preferences. The following section discusses experiences in enforcement that have implications for this comparative landscape.

## VII. ENFORCEMENT & CASE LAW LESSONS

### A. Indian Enforcement – *Sahara India* Case Study

A foundational enforcement case is *Sahara India Real Estate Corp. Ltd. (2012) 10 SCC 603 v. Securities and Exchange Board of India*. In that case, two companies of the Sahara group collected money from

[39] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, IFSCA (Aug. 7, 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf.

[40] Sidley Austin LLP, *Singapore Investment Management Regulatory Update (July 2025)*, Sidley Insights (July 3, 2025), https://www.sidley.com/en/insights/newsupdates/2025/07/singapore-investment-management-regulatory-update-july-2025#:~:text=In%20line%20with%20recent%20global,Singapore%20and%20authorized%20by%20MAS.

[41] Dubai Financial Services Authority, *Funds in the DIFC* (Sept. 14, 2014), https://www.dfsa.ae/application/files/4815/8220/1483/FUNDS-in-the-DIFC-Sep-14-2014.pdf.

[42] Guilhèm Becvort, *Luxembourg's Push for Private Capital Attractiveness and Competitiveness*, White & Case (Sept. 9, 2025), https://www.whitecase.com/insight-alert/luxembourgs-push-private-capital-attractiveness-and-competitiveness.

[43] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, IFSCA (Aug. 7, 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf.

Indian investors through "Optionally Fully Convertible Debentures" (OFCDs) that were not publicly offered in compliance with the SEBI requirements. The Supreme Court held that these issuances were indeed a public offering under the Companies Act and the SEBI Act, and ordered that Sahara refund the money to the backers. Sahara India defined offshore structures as not being leveraged to escape India's securities regulations. It exemplified the broad reach of regulation: even though SEZ entities initiated the transactions. It sold OFCDs across India, intersecting with a foreign vector, the court held that the jurisdiction of the SEBI encompasses the need to protect domestic investors. The judgment engendered a strong notion of investor protection and full disclosure. It provides a warning in light of GIFT IFSC: if fund managers in IFSC utilise offshore schemes directed at Indian investors, they must comply rigorously with the norms of IFSCA. Similar offshore schemes cannot escape the registration requirements governing schemes directed towards investors in India solely because the offshore scheme was not offered within the Indian mainland. The judgment led SEBI to impose multi-crore penalties on Sahara entities for "violating laws that govern fund-raising by corporates" for offering OFCDs and not complying with disclosure requirements. (**Case Study**: *Sahara India Real Estate Corp. Ltd. v. SEBI* The Supreme Court determined that Sahara's issuance was illegal, OFCDs were illegal public offerings, and ordered a refund to investors.[44] This landmark ruling confirmed the domestic securities law's applicability over cross-border fundraising initiatives to Indian residents. The key principles - strict compliance and strict disclosure obligations - are directly relevant for the funds in GIFT City).

**B. International Enforcement – Rule of Law for Funds**

Scandals in cross-border finance have resulted in more vigorous enforcement abroad. Recent examples include the SEC charging Centerline Investment (an investment adviser based in Hong Kong) in late 2024 for violations of Reg. M (shorting prohibited securities in the public offering context). Even though Centerline was not a traditional fund-structure scenario, it is relevant here because it demonstrates that regulators presented evidence of extraterritorial enforcement: Centerline was a non-U.S. operator that the SEC claimed manipulated the market concerning U.S. offerings[45]. Likewise, financial authorities in Singapore and Hong Kong have punished fund managers for deficiencies in custody or AML controls involving jurisdictional geography (e.g., SFC fines resulting from internal control deficiencies). This highlights the aggressive regulatory position by institutions to punish firms outside their jurisdiction that do not follow the local laws.

---

[44] *Sebi Fines 2 Sahara Cos ₹12 Crore*, *Times of India* (June 28, 2022), https://timesofindia.indiatimes.com/business/india-business/sebi-fines-2-sahara-cos-12-crore/articleshow/92500392.cms.

[45] Securities and Exchange Commission, *In the Matter of Centerline Investment Management Limited*, Exchange Act Release No. 34-101133, Admin. Proc. File No. 3-22156 (Sept. 23, 2024), https://www.sec.gov/enforcement-litigation/administrative-proceedings/34-101133-s.

Inside India, SEBI's recent fund-related enforcement underscores the importance of transparency. For instance, SEBI's AIF regulator has started litigating cases where fund managers have exceeded investment limits or delayed winding up expired AIFs -there has also been scrutiny in the market for features of master–feeder and CLO structures for possible regulatory arbitrage. Though the AIF and recent SEC enforcement do not take place under IFSCA jurisdiction, these types of enforcement actions signal the nature of issues pending or on the minds of IFSCA related to enforcement in the GIFT City. It is also important to note that IFSCA's mandate under Sections 13-14 of the Act provides it with enforcement authorities somewhat akin to SEBI, RBI, etc. IFSCA's enforcement actions may also involve coordination with Indian courts and regulators when needed.

From the Sahara to the recent SEC enforcement action, enforcement case law aims to educate fund managers and other GIFT City businesses on two points. First, GIFT City funds and companies must adopt strong compliance cultures. And complete transparency must be exercised in all disclosures to avoid litigation or penalties. Second, the regulatory perimeter is genuinely global, meaning one jurisdiction's regulatory violations can trigger responses and regulatory enforcement from other jurisdictions, including but not limited to any affected jurisdiction. GIFT City is a desirable, flexible jurisdiction; however, that does not mean "no enforcement." IFSCA has already signaled, during the still-modern era of newly-established and rapidly-evolving regulation, that AML/CFT and market conduct (e.g. recent guidance on suspicious transaction reporting) are a very high priority for enforcement in the GIFT City. Therefore, FMEs should be mindful of and guided by relevant precedents being issued globally.

### C. Strategic Implications: Positioning GIFT City in a Tariffed World

The previous discussion spells out challenges and opportunities for GIFT City. It raises crucial strategic work that GIFT has to do: the need to harness the strengths available in India, while balancing the global competitive environment.

1. **Global Diversification of Exports with GIFT's Role:** India has significantly limited exposure to the US slowdown, as the economy is less trade dependent. In fact, growth forecasters (IMF, ADB) have mostly retained healthy growth prospects for India, indicating that a domestic consumption boom and continued service export demand will offset weak manufacturing demand.[46]. Given this macro perspective, GIFT can certainly benefit: investors around the globe view India as a "key growth engine", and its direct exposure to new tariffs is limited. One report cites explicitly that investors "finally began upgrading India's sovereign rating, because tariffs on exports to the US would be manageable had significant reliance on

[46] Ramachandran, *supra* note 3.

trade". GIFT City can emphasise macro stability: funds placed in GIFT City would harness a 4-7% growth engine story in India within a relatively stable rule framework.

2. **Capital Inflows and Investor Shifts:** With that being said, the tariff war does create an additional layer of risk awareness to institutional investors. Investors may go to witness political neutrality. India's lack of alignment (and GIFT City's ability to form its legal framework) could be understandably advantageous to its future role in fintech and funds. Recent jumps in GIFT commitments suggest firmly that increased investor confidence exists.[47]. If enough companies transfer portions of their market presence from China to India or South Asia, this will create further demand and offer opportunities in this area. However, the Tax/Gift Phase requires Indian authorities to continue capitalising on the waterfall and renew market infrastructure (e.g., investor grievance mechanisms offer various means of faster resolution) if trust can be retained.
3. **Competitor Benchmarking:** GIFT will compete with Singapore, DIFC/ADGM, and other IFSCs in growth mode. Singapore's designation as the top financial centre in Asia shows its attractiveness.[48] In GIFT's case, GIFT can market its unique selling propositions: access to onshore markets, a single regulatory authority, and transparency (e.g., guaranteed 10% scheme tax rate for 10 years). The forthcoming EU-India FTA is another component: Europe-origin capital could enter GIFT's deals once completed. Co-investment and innovation funding (e.g., provincial entities for single-asset deals) appeals to global private equity/venture capital firms looking to co-invest in Indian startups.
4. **Regulatory Efficacy:** The 2025 Regulations and related reforms (e.g., third-party service providers) allow IFSCA a marketing opportunity for GIFT as a business-friendly entity. Rapid licensing of 177 FMEs by mid-2025 demonstrates being responsive. An ongoing series of dialogues with stakeholders (IFSCA's "Chintan Shivir" industry dialogues) shows IFSCA is listening to the industry. Equally, GIFT's regulators must commit to staying consistent and predictable. For example, any future replacements to the tax regime (e.g., 2030 special tax regime) should have been the subject of a significant notice period. Aligning with international AML/CFT standards (such as with MAS and ADGM) will give legitimacy to foreign investors, who may be concerned about compliance risk.

---

[47] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, IFSCA (Aug. 7, 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf#:~:text=Union%20Budget%20for%20FY%202023%E2%80%9324%2C,incorporate%20measures%20towards%20investor%20protection.

[48] *Singapore Overtakes Hong Kong to Become Asia's Top Financial Center*, Registration China (May 31, 2024), https://www.registrationchina.com/articles/singapore-overtakes-hong-kong-to-become-asias-top-financial-center/.

5. **Risks to consider:** Finally, GIFT has specific exposure to risks. The onshore-offshore model means the GIFT funds' returns are moving within the Indian home-market environment. By extension, the returns are also exposed to any domestic political, regulatory, or currency risk. If India's economic reforms begin to fade or some volatility comes, foreign funds will first weigh whether to engage the market or move cautiously. Therefore, the GIFT's regulations must include some intended protection (e.g., currency hedging rules that are easy to understand, repatriation easy to follow, and a dispute resolution process). Compared to Singapore or Luxembourg, where there is a well-trod legal recourse, GIFT is developing its jurisprudence; therefore, in many legal areas, policymakers should be particularly focused on providing some legal certainty (e.g. cross-border treatment of insolvency provisions for IFSC-regulated entities). This becomes important in developing investor confidence.

In aggregate, the US tariff war has sharpened thinking about a diversified Asia. GIFT city stands to capture a share of this shift, provided the Indian sub-continent macro strengths and constant regulatory fine-tuning are maintained. The volumes growth figures at a 40% quarterly increase in new commitments expected by mid-2025,[49] is indicative of the momentum, but maintaining it matters, so we will turn next to considerations for concrete policy suggestion determination so that GIFT City can realise its strategic objectives.

### D. Policy Recommendations and Future Roadmap

Expanding on the previous analysis, we suggest several policy interventions to boost the fund management ecosystem at GIFT City. The following recommendations are designed to align incentives, close remaining gaps, and future-proof GIFT against global standards and evolution:

1. **Improved Tax Certainty:** While GIFT funds benefit from a favorable 10% tax regime, it is worth noting that this is limited to a 10-year sunset. Policymakers should consider long-term tax stabilisation/extension of incentives to signal their commitment to the market. Doing so would signal commitment to the market, particularly if the pass-through status on Category III IFSC funds were to occur (as intended) on level terms with onshore AIFs. Further, continuing the tax neutrality on fund transfers would give further assurance to investors in their base fund, etc. (carve-out in the Income Tax Act)[50] and ensuring no retrospective changes would further reassure global investors.

---

[49] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, IFSCA (Aug. 7, 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf#:~:text=Union%20Budget%20for%20FY%202023%E2%80%9324%2C,incorporate%20measures%20towards%20investor%20protection.

[50] Athul Kumar, *et al.*, *Fund Formation: Attracting Global Investors — Global, Regulatory and Tax Environment Impacting India Focused Funds* (Nishith Desai Associates, Feb. 2024),

2. **Licensing and Ongoing Compliance Work-Load:** IFSCA has already decreased workload within the form-filling (e.g. 50% fees on re-filed PPMs) [51] and merged regulator coordination (via SEBI *vis-a-vis* NRIs )[52]. This workload reduction should be digitised and made transparent. For instance, a single-window platform will improve efficiency in FME registrations and scheme approvals, including clear timelines. Various other jurisdictions have established umbrella licenses for family office GP/LP/fund structures, which may broadly attract global fund groups. There may also be an opportunity to periodically test fund structure and other relevant products in a controlled environment (i.e., "regulatory sandboxes").
3. **Increase Fund Vehicle Options:** While the draft proposal on VCCs is welcome, IFSCA should accelerate the proposal's passage. Enabling Variable Capital Companies (open- and closed-ended) may start to level the field with competitors and attract Hong Kong or European managers familiar with that legal form. Additionally, IFSCA could enable real-estate investment trusts (REITS) to be private, commodity funds (to aid India's aspiration of becoming a bullion hub), and a fund vehicle with debt-personas for a niche market.
4. **Investor Protection and Transparency**: Building trust is paramount. It would be ideal for IFSCA to adopt and publish a code of conduct and/or best practices type publication (similar to MAS's LFMC guidelines) to promote best practices and develop an environment of investor trust. For example, establishing rules around conflict-of-interest issues (GP co-invest disclosure), side-letter disclosures, and segregation requirements would demonstrate a commitment to transparency, as that is the global norm. Encouraging or mandating third-party valuations and audits would promote investor confidence, similar to Luxembourg, which requires an AIFM for its RAIF. Regular (weekly or monthly) enforcement notices or summaries (or reports) to indicate the relevant authority will enforce the rule of law (similar to MAS's enforcement notice summary) would also engender a belief that there is some commitment to the rule of law.
5. **Global Integration and Marketing**: GIFT City must be internationally marketed. For example, if fund managers or products were offered reciprocal recognition (MOUs with either MAS/DFSA regulators), that could lead to increased cross-listings and fund flows. The

https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Fund-Formation-Attracting-Global-Investors.pdf.

[51] International Financial Services Centres Authority, *Transition to IFSCA (Fund Management) Regulations, 2025*, Circular F. No. IFSCA-IF-10PR/1/2023-Capital Markets/7 (Apr. 8, 2025), https://ifsca.gov.in/Document/Legal/transition-to-ifsca-fund-management-regulations-202508042025093121.pdf.

[52] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, IFSCA (Aug. 7, 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf.

suggested passports for UAE-India (or EU-India) fund structures should include the IFSC. Additionally, participation in international financial initiatives (such as IMF/OECD working groups on funds) would keep the IFSCA updated on fund changes and innovations. Finally, the GIFT was able to play on India's strong record with financial inclusion and fintech in relation to funds (APIs or blockchain for fund transaction processing or documentation). In that case, that could be appealing to more technology-savvy global investors.

6. **Leverage Domestic Institutional Investors**: Institutional investments in alternative assets in India's pension and insurance sectors are negligible[53]. Policies encouraging qualified domestic investors in India to park their capital in gifting specific types of funds with tax breaks or matching grants could increase their base capital and reliance on funding flow from abroad. This approach is similar to or a reaction to the measures in similar countries highlighted above (for example, the EPF and allocation amounts to local funds in Malaysia, etc.).
7. **Refining the Regulations**: IFSCA should ensure that FM regulations are reviewed routinely (e.g., in a 2-to 3-year cycle) and include feedback on the implementation challenges. When experience demonstrates that an aspect of the regulation (e.g. capital requirements or restrictions on investment outside of India) is too restrictive, the rules should be amended promptly once the experience is available. Anticipating global trends (thinking about ESG fund level standards, or crypto-asset level regulations) and developing anticipatory regulation as applicable will ensure that GIFT stays ahead of the curve.

By accepting this approach to governance, the policymakers can ensure that GIFT City can survive and thrive in an uncertain trade environment. The aim should be to make the regulatory process as streamlined as possible, without impeding governance. The balance between making it easier to do business within the coming days and governance has made hubs like Luxembourg and Singapore the hubs they are, and ought to be the goal of GIFT City.

## VIII. CONCLUSION

India's GIFT City is rapidly emerging as a dynamic International Financial Services Centre (IFSC) due to a coherent policy and solid growth metrics. The introduction of new IFSCA (Fund Management) Regulations, 2025, shows India's desire to fine-tune this ecosystem to include the best practices from throughout the world. In the meantime, uncertainty created by the US-China tariff war and geopolitical upheaval has reaffirmed the need to develop alternative financial centres.

[53] Kumar, *supra* note 50.

The GIFT City stands to benefit from some of the shifts it provides stable governance and access to India's large market already, and it is already beginning to see some fund commitments[54].[55]
However, being competitive will depend upon execution. Widening the comparison indicates that GIFT must continue to innovate – bringing the structure of Variable Capital Companies, global standard investor protections, and marketing itself as an efficient asset management hub. Enforcement and legal clarity (as cases regarding Sahara India have indicated) must be present and consistent to sustain investor confidence. Depending on how trade policies shift perceptions of risk around capital flows, India finds itself at a unique intersection, as pressure in the West or conflicts with China push capital out of both regions, GIFT can assert itself as a compelling, non-Western, Asian alternative.
In conclusion, the GIFT City model–based on the 2025 regulations–is well positioned to thrive in a "tariffed world," if it builds on India's growth story and adopts a mix of international fund management practices and norms. Policymakers should constructively build on recent reforms, add institutional support and remain conscious of real-time developments worldwide. GIFT City's objectives will be achieved if these measures are completed, and India will become a more significant player in global finance.

[54] International Financial Services Centres Authority, *Statistics for Fund Management Activities in GIFT IFSC as on December 31, 2024*, IFSCA (Aug. 18, 2025), https://ifsca.gov.in/Common/PreviewPdf?id=21626bde60601ef44a0ed02201817bb7&fileName=Statistics_for_Fund_Management_activities_in_GIFT_IFSC_as_on_December_31__2024_20250818_0549.pdf#:~:text=Number%20of%20Fund%20Management%20Entities,principle%20approvals.
[55] International Financial Services Centres Authority, *Fund Management Ecosystem at GIFT-IFSC Records Robust Growth Amid IFSCA's Progressive Regulatory Reforms*, IFSCA (Aug. 7, 2025), https://ifsca.gov.in/CommonDirect/ViewFile?id=21626bde60601ef44a0ed022016f9fa2&fileName=Fund_Management_ecosystem_at_GIFT_IFSC_records_robust_growth_amid_IFSCA%E2%80%99s_progressive_regulatory_reforms_20250807_0623.pdf#:~:text=Union%20Budget%20for%20FY%202023%E2%80%9324%2C,incorporate%20measures%20towards%20investor%20protection.

*This page is intentionally left blank*

Nupur, *Code, Credit, and Control: Recalibrating RBI's Digital Lending Directions, 2025 Between Innovation and Accountability,* 12 (1) SCHOLASTICUS 1 (2025).

# CODE, CREDIT, AND CONTROL: RECALIBRATING RBI'S DIGITAL LENDING DIRECTIONS, 2025 BETWEEN INNOVATION AND ACCOUNTABILITY

*Nupur*[*]

*ABSTRACT*

*The Reserve Bank of India's Digital Lending Directions, 2025, consolidate earlier guidelines into a unified framework aimed at protecting borrowers while supporting fintech innovation. These rules impose strict transparency and conduct standards that regulated lenders (banks, NBFCs, cooperative banks, and All-India Financial Institutions) must now enter formal contracts with their fintech partners (Lending Service Providers, or LSPs) and conduct robust due diligence. Borrowers gain standardised disclosures (Key Fact Statements with APR, fees, and terms) before loan acceptance, a mandated "cooling-off" right (minimum 1 day) to exit a digital loan without penalty, and grievance channels (RE and LSP nodal officers, RBI complaint portal). Crucially, data and app rules protect privacy; only minimal borrower data may be collected with explicit consent, digital loan apps (DLAs) must be registered, and all borrower data must reside in India (any overseas processing to be deleted within 24 hours). Simultaneously, multi-lender marketplaces must display all matched and unmatched offers impartially (no biased ranking or "dark patterns" allowed). This article analyzes these innovations, reviewing the new Directions' provisions, comparing them with global norms (e.g. EU withdrawal rights, UK "positive friction" in loan apps), and assessing their impact. We identify gaps (e.g. the exclusion of Buy-Now-Pay-Later products, ambiguities in practice) and propose suggestions (such as clarifying hybrid credit models and extending safeguards) to ensure the regulatory balance truly fosters safe, inclusive digital credit. In sum, the 2025 Directions mark a nuanced recalibration of India's lending landscape, layering accountability onto innovation, but their ultimate efficacy will hinge on clear guidance and enforcement.*

**Keywords**: Digital lending; RBI 2025 Directions; fintech regulation; consumer protection; credit innovation

[*] Nupur is a Student at Christ (Deemed to be University), Delhi NCR, India, and can be contacted at nupur[at]law[dot]christuniversity[dot]in

## I. INTRODUCTION

Digital lending has surged in India, using smartphone apps and online platforms to extend instant credit. While this has expanded access (especially for underbanked consumers), it also unleashed risks, hidden fees, opaque "dark patterns," exorbitant interest, aggressive collections and data misuse. In response, the RBI undertook a careful review[1]. A high-level Working Group (2021) "adopted the approach of striking a balance between boosting innovation in financial services and ensuring the orderly development of the growing market"[2]. Building on this, the RBI on May 8, 2025, released its Digital Lending Directions, 2025.[3] These directions consolidate earlier circulars (2020, 2022, 2023)[4] into a single framework, extending consumer safeguards without discarding digital credit channels. Crucially, the RBI explicitly states it "encourages innovation in financial systems,"[5] even as it targets abuses (mis-selling, data breaches, unethical recoveries) that had undermined trust[6].

This paper provides a comprehensive analysis of the 2025 Directions. We first outline the key legal features, definitions, scope, and obligations for lenders and fintechs. We then examine consumer protection enhancements, standardized disclosures (Key Fact Statements (KFS)), mandatory grievance mechanisms, cooling-off rights, and strict data-privacy rules[7]. Next, we discuss how the framework affects credit innovation, multi-lender marketplaces and app ecosystems versus the new compliance costs. We place India's approach in comparative perspective (comparing, for example, with EU and UK rules on digital credit). We identify gaps and ambiguities (e.g. the exclusion of BNPL and hybrid products) and conclude with constructive suggestions for regulators and industry. The 2025 Directions mark a watershed in Indian fintech law, seeking to balance consumer rights and the future of digital credit and understanding their strengths and limits is critical for policy-makers and lenders alike.

---

[1] CTR. FOR INTERNET & SOC'Y, DIGITAL LOAN APPS AND CONSUMER HARASSMENT: EVIDENCE AND POLICY RESPONSES (2022).

[2] Reserve Bank of India, *Report of the High-Level Working Group on FinTech / Digital Lending* (RBI Working Group report, 2021).

[3] Reserve Bank of India, *Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps* (Nov. 2021).

[4] Reserve Bank of India, *Master Direction / Circular: Loans Sourced by Banks and NBFCs over Digital Lending Platforms* (June 2020).

[5] Reserve Bank of India, *RBI Speech(s) and Governor Remarks on Fintech Regulation and Innovation* (various speeches, 2021–2025).

[6] P. Dasari, *Digital Lending in India: Harassment, Settlements, and the Regulatory Response*, SSRN (2024/2025).

[7] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

## II. KEY FEATURES OF THE RBI'S DIGITAL LENDING DIRECTIONS, 2025

The 2025 Directions establish a unified legal framework for any loan originated or serviced through a digital channel by a regulated entity (RE). In scope are all Indian commercial banks, cooperative banks, NBFCs/HFCs, and even All-India Financial Institutions when they lend via apps or platforms (excluded are credit card EMI schemes, merchant BNPL products, and P2P lending). Major elements include:

### A. Expanded Regulated Perimeter

The Directions adopt broad definitions. A Digital Lending App/Platform (DLA)[8] covers any mobile/web interface enabling lending. A Lending Service Provider (LSP) is any fintech or intermediary assisting the lender. Critically, even if lending is outsourced, the regulated lender (RE) retains full liability for compliance. The RBI now requires formal contracts with each LSP, detailing roles, recovery practices, audit rights, etc. Live registers of all LSP partnerships must be maintained, and annual "fit-and-proper" checks conducted. In effect, the Rules close loopholes, no informal "handshake" deals or secret fee-sharing (the RE remains "fully responsible and liable" for its LSP's actions).[9]

### B. Multi-Lender Platforms (Marketplace Neutrality)

Recognizing the rise of loan aggregators, the RBI now explicitly governs platforms with multiple lenders. LSPs running such marketplaces must display all loan offers matching a borrower's request, including offers from lenders who decline the loan. Each offer must show the lender's name, APR (with penal charges), tenure, EMI amount and fees. Critically, ranking or UI design must be unbiased, not using algorithms or "dark patterns" to nudge the borrower toward a particular loan (publicly disclosed rankings based on objective metrics are permitted). This ensures an apples-to-apples comparison, preventing aggressive steering. These neutralization requirements (effective Nov. 1, 2025) promote competition by making markets more transparent.

### C. Loan Disbursement and Repayment Rules

The RBI imposes strict "direct flow" of funds. All disbursements must go straight into the borrower's bank account. No third-party or LSP accounts may be used, except for narrow exceptions (e.g., co-lending joint accounts or direct-to-beneficiary schemes). Similarly, repayments must go directly to the lender (RE). No pass-through via LSPs or escrow is allowed. By eliminating middlemen in the money flow, these rules close earlier loopholes where LSPs could divert or delay funds, and ensure clear audit trails.

---

[8] Reserve Bank of India, *Master Direction – Digital Lending Directions, 2025* (RBI/DLD/2025-26/01).

[9] Reserve Bank of India, *On Outsourcing and Third-Party Management: Master Direction(s)/Circulars on Outsourcing of Financial Services* (relevant RBI outsourcing master direction, various dates).

### D. Borrower Screening

The Directions reaffirm that REs must assess each borrower's creditworthiness in every case (at a minimum collecting age, income, occupation). Importantly, a lender may not auto-escalate credit limits. Any increase requires an explicit borrower request and evaluation. This prevents unseen loan expansions via app interfaces. These provisions build on earlier RBI circulars on fair underwriting.

### E. Customer Disclosure and Grievance

Transparency is at the core. All loans must be accompanied by a Key Fact Statement (KFS), an RBI-standard form detailing APR, tenure, EMIs, all fees and penalties before the borrower accepts the offer.[10] The final sanction letter and terms (digitally signed) must then be emailed or messaged to the borrower. Lenders must also publish on their websites the list of digital loan products, LSP partnerships, and complaint channels (including RBI's Complaint Management System and "Sachet" portal). Additionally, both the RE and any interfacing LSP must each designate a nodal grievance officer, with contact info on the app and website. Borrowers can escalate unresolved complaints to the RBI's ombudsman if not settled in 30 days. These steps aim to eradicate hidden charges and ensure borrowers know where to seek help.

### F. Cooling-Off Period

A novel "exit" right is introduced. Borrowers receive a short cooling-off window (minimally 1 day, as determined by the lender's board and disclosed in the KFS) during which they can cancel the loan. They owe only the principal and a proportionate APR (no penalty) to walk away[11] (lenders may retain a reasonable one-time processing fee if disclosed upfront). This feature is akin to a consumer's right of withdrawal on distance credit contracts, allowing reflection after electronically signing. The Directions cut the previous minimum (3 days for longer loans) down to 1 day for all loans, streamlining the rule. The cooling-off right materially strengthens borrower autonomy post-sanction.

### G. Data and Technology Requirements

Echoing India's new data protection ethos, the RBI tightly curbs how apps use personal data. Lenders/LSPs may collect only the information necessary for credit evaluation, and only with explicit consent. Access to device resources is severely limited; apps cannot crawl contacts, call logs, messages, files, media, etc., except for a one-time need for KYC. All borrower data must be stored in India. If any processing occurs abroad, that data must be repatriated and deleted from foreign servers within 24 hours. Lenders must have comprehensive, public privacy policies

[10] Reserve Bank of India, *Master Direction / Consumer Protection Measures applicable to Regulated Entities* (consolidated consumer protection direction referenced in 2025 Directions).
[11] Regulation 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

disclosing any third-party data sharing.[12] These rules align digital lending with the Digital Personal Data Protection Act 2023[13] and CBPA's November 2023 guidelines, reflecting global privacy norms. On cybersecurity, too, REs/LSPs must meet RBI and CERT-in standards.[14]

### H. Default Loss Guarantee (DLG) Framework

The RBI also refines its first-loss guarantee rules. Only LSPs incorporated as companies (not individuals) may provide a default-loss-guarantee to lenders, and only to another REs or LSPs. A guarantor may cover at most 5% of an NBFC's disbursed loan portfolio. Guarantees cannot be invoked for revolving credit or any loans under government guarantee schemes. RBI specifies permitted forms (cash deposit, lien-marked FDR, or bank guarantee) and requires invocation within 120 days of default.[15] These constraints seek to prevent evergreening of loans (artificially hiding NPAs) while still allowing modest risk-sharing where appropriate.

### I. Reporting Requirements

Finally, the Directions greatly expand reporting. All loans originated via DLAs must be reported to credit information companies (building borrowers' credit histories).[16] Critically, from June 15, 2025, every DLA (even third-party apps) must register on RBI's Centralised Information Management System (CIMS) portal.[17] Chief Compliance Officers of REs personally certify this data's accuracy. The RBI will publicly list the registered apps (with the caveat that listing ≠ endorsement). By bringing all digital channels into view, RBI claims a de facto oversight loop on fintech apps that otherwise operate off-registry.[18]

Together, these rules constitute a stringent compliance regime. They notably enhance existing obligations (e.g., formalizing practices banks already follow) and introduce new ones (e.g. app registration, cooling-off).

## III. CONSUMER PROTECTION ENHANCEMENTS

A central aim of the 2025 Directions is to fortify consumer safeguards. Many measures align with international best practices in responsible lending:

---

[12] Ministry of Electronics & Information Technology (MeitY), *Rules under the Digital Personal Data Protection Act, 2023* (2023–2024).
[13] The Digital Personal Data Protection Act, No. 22 of 2023, *Gazette of India* (Aug. 11, 2023).
[14] European Banking Authority (EBA), *Guidelines on Outsourcing & ICT Risk Management* (EBA guidelines as comparative model for outsourcing/LSP chain oversight).
[15] RBI — *Circular / Clarification on Default Loss Guarantees & Risk-Sharing Arrangements in Digital Lending* (consolidated guidance, 2024–2025).
[16] Reserve Bank of India, *Notification — Registration / Listing Requirements for Digital Lending Apps (DLA) on CIMS* (June 2025 operational notice).
[17] Reserve Bank of India, *Guidance on Reporting of Loans to Credit Information Companies and Centralised Information Management System (CIMS) requirements* (2024–2025).
[18] Centre for Internet & Society, *Loan App Data Scraping & Privacy: An Analysis* (research brief/technical note).

### A. Transparency & Disclosure

The standardized KFS compiles all material loan terms in simple language upfront. Borrowers see APR, fees, tenure and penalties before accepting any offer, closing information gaps that fintech apps previously exploited. Emailed sanction letters and publicly disclosed privacy policies further guarantee borrowers know exactly what they are signing. In effect, borrowers move from opaque "consent screens" to crystal-clear fact sheets.

### B. Fair Marketing (No Dark Patterns)

Borrowers are shielded from manipulative UI/UX tactics. The RBI explicitly bans "dark patterns" on digital lending platforms, user interface tricks that mislead customers into high-cost loans. Similar concerns have arisen globally; for example, the UK FCA warns that some loan apps require "positive friction" to slow decision-making and prevent bypassing important information.[19] The RBI's rule, combined with requiring lenders' apps to be named and offering unbiased offers, means borrowers are less likely to be steered toward the costliest option.[20]

### C. Cooling-Off Right

This right is a powerful consumer tool. Analogous to the EU's 14-day credit withdrawal right and India's existing 1-3 days look-up periods, it creates a short "reflection window" after the contract. During the cooling-off period, a borrower who has second thoughts can terminate the loan by repaying only principal plus the proportionate interest accrued, with no foreclosure penalty. The RBI has consciously cut this window to 1 day (shorter than many earlier regimes) to balance lender certainty with consumer remorse options. This measure could prevent fraud or rash decisions: for instance, if a borrower found hidden fine-print after signing, she can effectively rescind the deal almost immediately.

### D. Grievance Redressal

The Directions institutionalize complaints handling. Both lenders and their fintech agents must have trained grievance officers, and their contact info must be clearly visible on loan apps and websites. If a borrower's complaint is unresolved in 30 days, the RBI system provides a fallback. Such multi-tier redress enhances accountability: lenders risk RBI penalties for unresolved grievances. These provisions bring digital credit in line with India's general consumer law trends.

### E. Data Privacy

Borrower data rights see a major upgrade. All data collection must be "purpose-specific" with explicit borrower consent, and borrowers may revoke consent at any time. Mobile resource access

[19] Financial Conduct Authority (UK), *Consumer Duty and Guidance on Digital Design / Online Journeys* (FCA publications/guidance on digital UX and "positive friction", 2023–2025).
[20] Academic article / conference paper on *dark patterns in fintech* (e.g., Mathur et al., *Dark Patterns at Scale: Findings and Implications*).

(e.g., contacts, SMS) is sharply curtailed. The Directions mirror the principle of data minimization in the new Digital Personal Data Protection Act. In practice, lenders and apps must rebuild their data practices; for example, if an app once scraped a borrower's contact list, it is now flatly prohibited.

### F. Credit Reporting

By mandating that all digital loans be reported to credit bureaus, the RBI promotes fair credit discipline. Every on-time or late payment gets recorded, helping responsible borrowers build a score and penalising willful defaulters. This aligns with full-file reporting laws in places like Australia. Notably, India chose not to exempt microloans here (unlike Kenya's rule allowing very small defaults to slip to protect poor borrowers). The RBI evidently prioritises creating comprehensive credit histories for digital borrowers.

Overall, consumers gain from these rules. As one analysis observes, "the new rules seek to balance innovation with integrity and ensure that the marketplace is safe and sound for consumers". The combined effect is a stronger safety net, greater up-front clarity (KFS), the freedom to exit bad deals, control over personal data, and enforced responsiveness by lenders. As a result, ethically questionable fintech practices should be curbed, making digital credit "inclusive, secure and sustainable".

## IV. IMPLICATIONS FOR CREDIT INNOVATION

While bolstering protections, the Directions also reshape the fintech credit landscape. Many provisions advance responsible innovation, but compliance costs may influence market dynamics. On the positive side, the Rules explicitly accommodate new lending models. The regulator's multi-lender platform rules recognize the reality of loan comparison apps, aiming to nurture a competitive marketplace. By requiring lenders to disclose offers impartially, borrowers can access a wider set of credit options. This transparency could deepen credit penetration; even reluctant borrowers may try digital loans if confident terms are fair. Moreover, clear rules on contractual arrangements and audit rights give banks and NBFCs confidence to partner with fintechs, potentially scaling up digital credit flow.[21] For example, an RBI-authorized co-lending or marketplace arrangement may now be more predictable for banks than before.[22]

However, industry commentators note the compliance burden is substantial. Lenders must overhaul systems generating KFS data before the borrower selects a loan, segregating funds flows, and overhauling UI/UX to eliminate bias. Fintech platforms face new documentation (contracts

[21] *NBFCs Face Provisioning Brunt as RBI Tightens DLG Norms*, Econ. Times , May 27, 2025.

[22] Centre for Financial Inclusion / academic piece, *Digital Credit Algorithms in India: Inclusion or Exclusion?* (policy brief / paper).

with each bank), IT work (automating KFS presentation and consent records), and legal exposure (their partner's CCO will sign off on regulatory compliance). Smaller startups may struggle to meet these requirements. Industry observers predict some consolidation, with only well-funded players absorbing the costs. In short, the "compliance bar" has been raised.

The RBI appears aware of this tension. Its preamble explicitly avoids "overhauling" the framework, instead "refining" it. By not imposing new interest rate caps and allowing flexibility (e.g. letting the RE's board fix the cooling-off length), the RBI tries not to stifle growth. Indeed, key voices praise the balance. One industry article notes the directions "encourage fintech-driven credit growth, but… do not tolerate predatory behavior".[23] Lenders can still innovate on credit-scoring, product design and delivery now within defined guardrails.

Data-driven innovation will also pivot. The strict localization and consent regime pushes fintechs to build India-specific data infra global cloud providers will need local deployment or data-delete flows. This is likely seen as a trade-off between protecting privacy and ease of cross-border development.[24] Conversely, richer credit data from mandatory credit bureau reporting (including the borrower's repayment history) should fuel better risk models. One effect previously unscored borrower may now generate on-time records, aiding machine-learning credit algorithms in scoring poor borrowers.

Finally, Fintech partnerships must be reframed. With REs liable for all LSP actions, banks will more tightly police their platforms. The scheme effectively "regulates fintech by proxy" The RBI sidesteps licensing non-banks, yet achieves oversight by enforcing contracts and audits. This creates an incentive for fintechs to adopt internal compliance (in data use, UI design and collections) as a survival strategy. Over time, one hopes this professionalizes the sector.[25]

Overall, the directions signal that innovation must proceed "with integrity." Borrowers stand to benefit from a clearer, safer market. Lenders and fintechs must respond by strengthening controls and retooling apps.[26] The net impact on credit availability remains to be seen in theory; reducing mistrust should expand uptake; in practice, higher costs may slow entry. The RBI's challenge will

[23] Bank for International Settlements (BIS), *Working Papers on FinTech Credit and Financial Stability* (BIS reports on fintech credit models and systemic implications).

[24] Legal firm commentary (e.g., AZB & Partners), *Practical Note on RBI Digital Lending Directions, 2025* (practitioner analysis).

[25] Cyril Amarchand Mangaldas, *RBI Consolidates Directions on Digital Lending: Implications for REs & LSPs,* India Corp. L. Blog (May 20, 2025), https://corporate.cyrilamarchandblogs.com/2025/05/fig-paper-no-44-series-3-rbi-consolidates-directions-on-digital-lending-implications-for-res-lsps/.

[26] AJ Yuan Chen, *et al.*, *Digital Lending and Financial Well-Being: Through the Lens of Mobile Phone Data* (Harvard Bus. Sch., Working Paper No. 23-076, 2023), https://www.hbs.edu/ris/Publication%20Files/23-076rev11-13-23_b3ecc663-8dbd-4446-9059-115f511e612c.pdf.

be to monitor implementation[27] and tweak rules as needed, ensuring innovation thrives under accountability.[28]

## V. INTERNATIONAL AND COMPARATIVE CONTEXT

India's 2025 framework reflects global trends in balancing fintech growth with consumer rights. Under the G20/OECD principles[29], financial regulators increasingly stress customer-centricity and information symmetry. A few illustrative parallels:

### A. European Union

EU consumer credit law (Consumer Rights Directive) grants borrowers a 14-day withdrawal right for distance loans, mirroring India's cooling-off concept. The forthcoming EU Digital Finance package will further tighten disclosures and ban unfair UI. Notably, EU data rules (GDPR) entitle loan applicants "not to be subject to a decision based solely on automated processing" and to obtain human review[30]. India's standards echo these values, it mandates human-friendly summaries (KFS) and gives borrowers control over app permissions.

### B. United Kingdom

The UK Financial Conduct Authority has similarly highlighted the need for transparency and positive design in online lending. A recent FCA review found many loan apps lack "positive friction" (such as time-delays or check boxes) that would pause customers and ensure they understand costs.[31] This matches RBI's ban on deceptive loan funnels.[32] The FCA also pursues full reporting to credit reference agencies. Like India, UK regulators see technology as a double-edged sword, necessitating design standards.[33]

### C. Australia and New Zealand

Regulators here mandate full-file credit reporting (each lender must share all consumer loan data).[34] This assists in affordability checks and deterring reckless lending.[35] India's requirement that all digital loans hit the credit bureaus is akin to this, though Australia additionally requires lenders to verify the loan purpose and customers' capacity to repay. On the data front, RBI's localization

---

[27] Reserve Bank of India, *FAQ: Digital Lending Guidelines* (RBI FAQ, 2023).
[28] International Telecommunication Union (ITU) / UNCDF reports on digital finance inclusion (contextual comparison).
[29] OECD, *Principles for Digital Financial Inclusion* (2016).
[30] European Commission, *Digital Finance Package / Proposals on Digital Finance (regulatory posture relevant to digital lending)* (2023–2024 materials).
[31] Financial Conduct Authority (UK), *Discussion Paper / Report on Lending Apps and Marketplaces* (FCA thematic review, 2023–2025).
[32] Bank of England / FCA joint papers on digital financial resilience (relevant thematic analysis).
[33] UK Consumer Credit Act 1974 (statutory background for UK consumer credit disclosure rules).
[34] Australian Treasury, *Review of Australia's Credit Reporting Framework* (Final Report / policy documents, 2023–2024).
[35] Australian Securities & Investments Commission (ASIC), *Responsible Lending Guidance and digital credit materials* (ASIC guidance on digital lenders).

requirement contrasts with the open-data pushes seen in some markets (e.g., open banking), but aligns with many emerging markets, RBI's Digital Lending Directions, 2025: Between Consumer Protection and Credit Innovation, data sovereignty moves.

### D. Kenya and Africa

Some African regulators focus on consumer risk. For instance, Kenya's digital credit rules prohibit lenders from reporting default on "nano" loans under ~$8[36], protecting very poor borrowers from blacklisting over trivial debts. India, however, chose not to include such an exemption, instead mandating that every digital loan be reported. This reflects a policy choice emphasizing credit discipline over targeted leniency. The RBI did adopt Kenya's idea of an electronic dispute resolution portal, but through its own CMS.

### E. United States

The U.S. has fewer digital lending-specific rules, but CFPB enforcement actions and state laws (e.g., California's ban on certain data uses) echo these concerns. For example, California law prohibits lenders from scraping borrowers' phones without consent, similar in spirit to RBI's app restrictions. Meanwhile, U.S. law also gives rights to explanations under the Equal Credit Opportunity Act (anti-discrimination) and requires Truth in Lending disclosures, conceptual cousins to the KFS.[37]

In sum, the RBI's framework is broadly in line with an international shift; regulators are no longer content with letting fintech happen unchecked. They're demanding that innovation respect transparency, fairness, and data rights. India's Guidelines stand out for their detail (e.g. app registry, explicit contract rules) and alignment with its new data law. However, India's fintech market also has unique features (e.g. Aadhaar/KYC, UPI ecosystems) that other countries lack. The directions thus blend global principles with India-specific fixes.[38]

## VI. GAPS, AMBIGUITIES AND CHALLENGES

Despite its strengths, the 2025 regime has notable lacunae and practical issues that warrant attention:

[36] Central Bank of Kenya, *Guidance on Digital Credit Providers* (CBK circulars and consumer protection guidance, 2019–2022).
[37] Consumer Financial Protection Bureau (U.S.), *Supervisory and Enforcement Actions related to Digital Lending* (CFPB briefs / enforcement summaries).
[38] Organisation for Economic Co-operation and Development (OECD), *Principles for Consumer Protection in the Context of Electronic Commerce / Digital Financial Services* (OECD policy guidance).

### A. Buy-Now-Pay-Later and Hybrid Credits

The Directions explicitly exclude "merchant BNPL" from their scope.[39] Yet BNPL is booming in India (often provided via fintechs without conventional loan paperwork). The RBI has separately clamped down on BNPL non-bank providers (as with the recent seizure of Simpl's payments functions). The NDTV analysis notes a gray zone hybrid model that blend BNPL mechanics with term loans may evade clear categorization. Without guidance, firms could structure products to avoid regulation. A constructive step would be for the RBI (or Finance Ministry) to clarify how these models will be treated, for example, requiring disclosures or registrations for large BNPL providers, or expanding the rulebook if BNPL products bear interest.[40]

### B. Multi-Tier LSP Chains

The Directions assume a simple two-tier (RE ↔ LSP ↔ borrower) structure. But what if an LSP further outsources KYC or tech services to another firm? Could a so-called LSP-of-LSP escape oversight? The NDTV article highlights this ambiguity.[41] The RBI may need to issue FAQs or a circular clarifying that only LSPs directly contracted by REs qualify, or that downstream providers must adhere to the same rules. Otherwise, operationalizing due diligence and accountability along supply chains will be tricky.

### C. Timing of Disclosures

In theory, KFS must be shown before the borrower picks a lender. But as one industry analysis points out, KFS data (APR, EMI) often depends on the specific loan offer. Practically, apps usually have customers choose an offer and then generate the KFS. How can this work? The NDTV analysis flags this as a conundrum.[42] RBI or industry guidelines may need to standardize the process (e.g. generate KFS on-the-fly as soon as any offers are computed, before final acceptance).

### D. Data Localization vs. Cloud Infrastructure

Requiring all borrower data to be stored in India (and cleaned from foreign servers) can be technologically challenging for lenders using global cloud services. While the intention is data security, in practice, this could slow down lenders migrating to big-data platforms or scaling risk models. Some industry experts have called for a phased approach (similar to India's earlier rules for payment data) to let larger players comply without service disruption.

### E. Scope of "Credit Innovation"

---

[39] The Times of India, *"RBI cracks down on 'Buy Now Pay Later'"* (press coverage of BNPL regulatory attention, 2024–2025).

[40] Bank for International Settlements (BIS), *Working Papers on FinTech Credit and Financial Stability* (BIS reports on fintech credit models and systemic implications).

[41] NDTV / Business News analysis, *Decoding RBI's Digital Lending Directions: Tightrope for Fintechs* (practitioner commentary, May 2025).

[42] World Bank/CGAP, *Digital Credit: Policy Guidance and Consumer Protection Considerations* (CGAP policy briefs).

The directions cover regulated financial institutions. What about pure fintech platforms that issue storefront loans (some P2P or social lending apps)? Since they would eventually need a bank partner, these regulations apply indirectly via the bank. Nevertheless, the RBI might consider whether high-volume fintech lenders should themselves be licensed (as NBFCs or otherwise), as suggested by some commentators.

### F. Enforcement and Remedies

The Guidelines rely on REs (and their officers) to enforce compliance. But if an LSP violates the law, for instance, by embedding a hidden fee, recourse ultimately is against the bank. It will fall on banks' compliance teams (or RBI supervision) to police the fintechs. This "indirect" approach may allow some unethical players to operate in the shadows. A possible remedy is empowering consumer authorities (like the CCPA or RBI Ombudsman) to penalize LSPs directly, even without RBI licensing powers.

In short, while the 2025 Directions greatly improve the rulebook, practical clarity and enforcement will determine their success. Stakeholders have called for RBI clarifications on these issues. It will be important for the RBI to issue FAQs or hold industry consultations to refine these gaps. Ideally, the RBI will monitor outcomes and update the framework in response to new fintech innovations, rather than let loopholes persist.

## VII. RECOMMENDATIONS AND POLICY SUGGESTIONS

Drawing on the above analysis and global practices, we offer constructive suggestions:

### A. Extend Consumer Protections to BNPL

Given the size of India's BNPL market and the recent regulatory focus on it, the RBI or Finance Ministry should consider amending the Directions (or issuing separate guidelines) to bring large BNPL schemes under similar disclosure and grievance norms. For example, any BNPL provider partnering with multiple lenders could be required to present a KFS (even for zero-interest installments) and register their apps as DLAs. Alternatively, RBI could push the Reserve Bank Innovation Hub (RBIH) to launch a code of conduct for BNPL.[43]

### B. Clarify Ambiguities via Formal Guidance

The RBI should quickly issue clarifications on key points, e.g. confirm that ranking neutrality means not suppressing lenders that have offers for the borrower, and explain how the KFS can be offered pre-offer. Providing annotated examples of compliant app flows (and "bad" ones) would

[43] Reserve Bank of India Innovation Hub (RBIH), *Discussion Paper / Sandbox Findings on Fintech-Bank Partnerships* (RBIH reports, 2022–2024).

help the industry align practice to intent. Ensuring fintechs know the boundaries fosters innovation within those lines.

### C. Risk-Based Compliance for Fintechs

To prevent stifling emerging startups, the RBI could consider a tiered compliance approach. Smaller platforms with, say, sub-XXX crore in loans per year might face simplified reporting or phased deadlines, whereas large aggregators must meet full obligations immediately. This is analogous to RBI's SB-4 (scale-based) NBFC norms. Such a gradation would allow nascent players to scale up without immediate full-scale licensing burdens, while still preserving core consumer rules.

### D. Strengthen Financial Literacy and Redress Awareness

As fintech grows, borrowers need education on digital credit. RBI, in partnership with DoT and consumer agencies, could run campaigns explaining the KFS and complaint mechanisms. At a minimum, guidelines could require that DLAs include FAQ or tutorial content on how to read the KFS and how cooling-off works. Empowered customers will use the protections (cooling-off, RBI complaint system) more effectively, reinforcing the rules' intent.

### E. Data Innovation with Safeguards

The RBI should coordinate with Data Protection authorities to harmonize the fintech data rulebook. Encouraging "permissioned" data sharing (e.g., via Account Aggregators) could let lenders access richer underwriting info (income accounts, bills) without violating consent standards. RBI might support open finance initiatives to foster innovation in credit scoring while preserving explicit user control.[44]

### F. Periodic Review of Outcomes

Finally, the RBI should treat these Directions as a living framework. After one year of implementation, the RBI could gather data on complaints, defaults, app registrations, and market structure changes. This evidence-based review could then inform tweaks (for instance, adjusting the cooling-off timeline if it causes operational issues, or revisiting APR rules if rates surge). International bodies like OECD[45] and AFI recommend such ongoing monitoring of consumer outcomes. By staying responsive, the RBI can ensure the balance between innovation and protection evolves properly.

## VIII. CONCLUSION

[44] Reserve Bank of India, Master Direction – Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, (2016).

[45] OECD / AFI policy brief, *Regulatory Approaches to Consumer Protection in Digital Finance* (policy recommendations).

The Reserve Bank's Digital Lending Directions, 2025, mark a watershed in India's fintech regulation. By layering detailed disclosure, data, and contractual requirements onto the digital loan process, the RBI has put consumer protection front-and-center while attempting to preserve digital credit channels. These rules, if effectively enforced, will reduce the murky "wild west" reputation of lending apps, shutting down exploitative practices and boosting borrower confidence.

At the same time, the guidelines do not halt innovation; they legitimize key fintech models (marketplaces, co-lending structures, digital wallets) within guardrails. As one commentary notes, the 2025 Directions seek to "balance innovation with integrity", encouraging growth but "not tolerating predatory behavior". In comparative terms, India has become one of the first major economies to comprehensively regulate app-based loans in this way. The approach aligns with global norms (EU, UK, OECD) while reflecting India's local context (e.g. strong data localization, Aadhaar-based KYC, UPI rail).[46]

Ultimately, the success of this regulatory recalibration hinges on clarity and enforcement. The RBI must promptly address the remaining ambiguities and ensure compliance without creating undue friction for genuine lenders. If implemented earnestly, the new Directions could achieve their dual aim of empowering consumers with transparency and rights, and empowering responsible lenders to innovate on a level playing field. In doing so, they set a template for a digital credit ecosystem that is both dynamic and durable, truly marrying consumer protection with credit innovation.

[46] World Bank / CGAP, *Policy Note: Responsible Digital Credit — Consumer Protections and Supervision* (CGAP/World Bank recommendations).

*This page is intentionally left blank*

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.

*This page is intentionally left blank*

Shivalik Pal & Mahak Khirwal, *Central Bank Digital Currencies & Cross-Border Payments: India's Digital Rupee Experiment in a Fragmented Global Financial Order,* 12 (1) SCHOLASTICUS 1 (2025)

# CENTRAL BANK DIGITAL CURRENCIES & CROSS-BORDER PAYMENTS: INDIA'S DIGITAL RUPEE EXPERIMENT IN A FRAGMENTED GLOBAL FINANCIAL ORDER

*Shivalik Pal[*] & Mahak Khirwal[†]*

*ABSTRACT*

*The proliferation of private digital currencies and stablecoin has compelled central banks worldwide to reassert monetary sovereignty through Central Bank Digital Currency (CBDC) initiatives. This paper examines India's Digital Rupee (e₹) within the broader context of global CBDC developments and cross-border payment infrastructure. Through doctrinal analysis and comparative methodology, we investigate India's hybrid CBDC architecture, its legal foundations under the RBI Act (1934) and related statutes and its positioning within emerging multilateral frameworks like mBridge.*

*India has processed over 2.73 crore retail CBDC transactions, demonstrating early adoption momentum. However, significant challenges persist like reconciling technological innovation with monetary sovereignty, ensuring cross-border legal certainty, and balancing financial surveillance with privacy rights. We analyse these tensions through comparative study of China's e-CNY, the Digital Euro, and BIS interoperability frameworks. Our findings suggest that India's tiered anonymity model and integration with digital public infrastructure ("DPI") offer a cautiously inclusive approach. Yet, without harmonized international legal standards, cross-border CBDC adoption risks deepening financial fragmentation rather than resolving it. The paper concludes with policy recommendations for statutory reform, data governance, and India's potential leadership in shaping Global South CBDC cooperation networks.*

**Keywords:** Central Bank Digital Currency, Digital Rupee, Cross-border Payments, Monetary Sovereignty, Financial Technology, RBI, Payment Systems.

[*] Shivalik Pal is a fourth year law student at National University of Study and Research in Law, Ranchi, and can be contacted at shivalik[dot]pal[at]nusrlranchi[dot]ac[dot]in

[†] Mahak Khirwal is a fourth year law student at National University of Study and Research in Law, Ranchi, and can be contacted at mahak[dot]khirwal[at]nusrlranchi[dot]ac[dot]in

# I. INTRODUCTION: THE DIGITAL CURRENCY MOMENT

## A. Post 2020 Trend in Digital Money

The global financial landscape has undergone profound transformation since 2020. The COVID-19 pandemic accelerated digitalization across payment systems, while simultaneously exposing vulnerabilities in traditional correspondent banking networks[1]. Private stablecoins, notably Tether (USDT), USD Coin (USDC), and Facebook's aborted Libra/Diem project[2] emerged as significant actors in cross-border value transfer, processing billions in daily transactions outside conventional regulatory perimeters. Decentralized cryptocurrencies like Bitcoin and Ethereum demonstrated persistent volatility[3], yet attracted institutional interest as alternative stores of value.

This proliferation of over 5,000 privately issued digital currencies since Bitcoin's 2009 launch[4] has prompted an unprecedented response from central banks. Over 130 countries representing 98% of global GDP[5] are actively researching or piloting CBDCs[6], with 44 already in advanced pilot phases[7]. The urgency stems not merely from technological competition but from fundamental concerns about monetary sovereignty, financial stability, and the state's role in money creation.

## B. India's Digital Public Infrastructure and the Digital Rupee Initiative

India's CBDC initiative is deeply embedded within its broader digital public infrastructure (DPI) strategy. The successful deployment of Aadhaar (a biometric identity system covering 1.3 billion residents), Unified Payments Interface (UPI, processing over 10 billion transactions monthly), and the India Stack framework has created a unique foundation for digital currency implementation[8]. The Reserve Bank of India's (RBI) launch of the Digital Rupee builds systematically on this infrastructure[9], aiming to address persistent gaps in financial inclusion while countering risks posed by unregulated cryptocurrencies. Its rollout is not merely technological but rooted in a layered statutory mandate that provides both authority and constraints. The RBI Act, 1934, particularly

---

[1] Vučinić, Milena and Radoica Luburić, *Fintech, Risk-Based Thinking and Cyber Risk*, 11 J. Cent. Banking Theory & Prac. 27 (2022).

[2] Ahmed Mahrous, et al, *Stablecoins: Fundamentals, Emerging Issues, and Open Challenges*, arXiv (2025), https://arxiv.org/abs/2507.13883.

[3] Cyrus Cole, *Institutional Adoption of Bitcoin and Ethereum ETFs: Reshaping Volatility and Unlocking Long-Term Value*, AInvest (Aug. 25, 2025), https://www.ainvest.com/news/institutional-adoption-bitcoin-ethereum-etfs-reshaping-volatility-unlocking-long-term-2508.

[4] List of Cryptocurrencies, *Wikipedia*, https://en.wikipedia.org/wiki/List_of_cryptocurrencies (last visited Oct. 19, 2025).

[5] Neha K. Chawla, *Implications of Central Bank Digital Currency in India: A Critical Analysis*, DME JOURNAL OF LAW (2023).

[6] Jianguo Xu, *Developments and Implications of Central Bank Digital Currency: The Case of China e-CNY*, Asian Economic Policy Review (2022).

[7] Atlantic Council, *Central Bank Digital Currency Tracker*, https://www.atlanticcouncil.org/cbdctracker (last updated July 2025).

[8] Ministry of Electronics and Information Technology, *India Stack Global – Digital India*, https://www.digitalindia.gov.in/initiative/india-stack-global (last visited Oct. 19, 2025).

[9] Reserve Bank of India, *Annual Report on Currency and Finance – Chapter I: India's Digital Revolution: Opportunities and Challenges*, RBI Publications (July 29, 2024), https://www.rbi.org.in/scripts/PublicationsView.aspx?Id=22457.

Section 22, establishes the central bank's exclusive power to issue currency, which has now been extended into the digital domain through Section 22A inserted by the Finance Act, 2022, giving explicit recognition to digital legal tender. Complementing this, the Payment and Settlement Systems Act, 2007 ensures that the Digital Rupee functions within India's regulated financial rails, while the Banking Regulation Act, 1949, defines how intermediary banks participate in the CBDC ecosystem. However, as India moves towards cross-border CBDC experimentation through platforms like BIS mBridge, the Foreign Exchange Management Act (FEMA), 1999, becomes central to determining the legal permissibility of holding and transferring Digital Rupee outside national borders. Simultaneously, the Digital Personal Data Protection Act (DPDP), 2023, introduces obligations of privacy, proportional data processing, and state accountability, making the design of Digital Rupee wallets a site of constitutional scrutiny.

Despite this robust statutory architecture, several legal and policy frictions remain unresolved. A primary tension lies between maintaining monetary sovereignty and enabling cross-border interoperability, especially as multilateral CBDC networks may require shared governance protocols. Equally significant is the challenge of balancing traceability requirements for anti-money laundering compliance with the right to privacy recognized under Indian constitutional jurisprudence. FEMA's current framework, built around conventional fiat and securities, lacks clarity on the legal status of CBDC once it leaves domestic jurisdiction or is held by non-residents. Moreover, as multiple countries pursue their own CBDC projects, the risk of fragmented bilateral arrangements looms large, raising the question of whether initiatives like mBridge will lead to true interoperability or simply a new layer of controlled financial blocs. Against this backdrop, the objective of this research is to critically examine the legal architecture of India's Digital Rupee within a comparative CBDC landscape, assess its cross-border, and data governance implications, and propose legal adjustments and multilateral coordination mechanisms necessary for a coherent and sovereignty-consistent CBDC framework.[10]




[10] K. M., Mahesh et al, *Impact of Centralized Blockchain Digital Currency (CBDC): For Financial Inclusion and Sustainability*, International Journal of Management, Technology, and Social Sciences (2024).

## II. UNDERSTANDING THE CBDC FRAMEWORK: CONCEPTS AND CLASSIFICATIONS

Central Bank Digital Currencies represent a sovereign digital form of money issued by central banks, distinct from both physical cash and commercial bank deposits. The Bank for International Settlements (BIS) classifies forms of money based on four dimensions: the issuer (central bank versus private entities), the form (digital or physical), the accessibility (restricted wholesale access or open retail access) and the technology underpinning it (either identity-linked account-based models or cryptographic token-based systems). The BIS "money flower" further refines this classification by examining whether the digital currency constitutes a direct claim on the central bank or an indirect claim via intermediaries, the level of anonymity permitted and the extent of peer-to-peer, offline transactional capability it enables[11]. These conceptual distinctions are critical for understanding different CBDC design choices adopted by jurisdictions.

CBDC architectures around the world vary significantly. Under a Direct CBDC model, the central bank maintains all customer accounts and processes all retail transactions, resulting in full monetary control but imposing heavy operational burdens and potential disintermediation of commercial banks[12]. In contrast, Hybrid CBDC models distribute operational responsibilities between the central bank and regulated financial intermediaries, allowing the central bank to retain control over the monetary base while delegating KYC, wallet management, and transaction processing to banks and payment service providers[13]. There also exists an Intermediated CBDC model where retail users hold claims through intermediaries rather than directly against the central bank, raising questions about legal enforceability and insolvency risk. A more experimental form, the Synthetic CBDC ("sCBDC"), allows private stablecoin issuers to offer digital tokens fully backed by central bank reserves. While this model promotes private innovation, it blurs the boundary between public and private money creation. India has clearly signalled preference for a Hybrid model[14], balancing innovation with regulatory oversight[15].

On the technological front, CBDC infrastructure can operate on permissioned distributed ledger systems or traditional centralized databases. Distributed ledger technology (DLT) offers auditability, verifiability, and cryptographic assurance while permitting controlled validator access.

---

[11] Bank for International Settlements, *Central Bank Digital Currencies*, CPMI & Markets Committee Rep. No. 174, at 4–6 (Mar. 2018), https://www.bis.org/cpmi/publ/d174.pdf.

[12] Milena Vučinić & Radoica Luburić, *Fintech, Risk-Based Thinking and Cyber Risk*, 11 CENTRAL BANKING THEORY AND PRACTICE J. (2022) at 27.

[13] Bank for International Settlements, *A Prototype for Two-Tier Central Bank Digital Currency (CBDC): Project Aurum*, BIS Other Publications No. 57, at 6–7 (Oct. 2022), https://www.bis.org/publ/othp57.pdf.

[14] Dr. Pragya Nayyar & Dr. Jasdeep Kaur, *Origin of CBDC in India: Prospects and Challenges of Issuance & Management*, 7 INT'L J. ADV. RES. COM. MGMT. & SOC. SCI. at 222, 224–26 (2024).

[15] Mahrous, *supra* note 2.

Systems like Hyperledger Fabric and R3 Corda are actively explored in pilot environments, especially for wholesale interbank settlements. Conversely, centralized database infrastructure, with higher throughput and easier integration into existing core banking systems, is currently preferred for retail CBDC pilots due to efficiency and lower energy consumption[16]. India follows a pragmatic, technology-neutral stance, allowing infrastructure to vary depending on use-case requirements, including hybrid architectures combining centralized core systems with DLT features where needed.

Access mechanisms further shape CBDC design. Account-based CBDCs rely on identity authentication for every transaction, ensuring strong KYC and AML compliance but increasing surveillance risks.[17] Token-based systems, on the other hand, validate ownership through cryptographic keys rather than identity, enabling cash-like peer-to-peer offline transfers and greater privacy but complicating regulatory oversight[18]. India has adopted a tiered hybrid access model[19][20] that calibrates user anonymity and KYC stringency based on transaction value and risk category, allowing limited pseudonymity for low-value transactions while enforcing full transparency for high-value transfers.

The legal classification of CBDCs remains a developing area. Some jurisdictions define CBDCs explicitly as fiat currency backed by sovereign guarantee,[21] while others classify them as legal tender with mandatory acceptance for debt settlement[22]. A key legal distinction is whether CBDC constitutes a direct liability of the central bank, which ensures depositor protection even if intermediaries fail. While some scholars argue CBDCs could be regulated as financial instruments[23], India has taken a clear position by treating the Digital Rupee as currency under the RBI Act framework rather than a security or payment instrument under financial market

[16] Harsh Khandelwal et al., A Survey on Central Bank Digital Currency (CBDC) Implementation Using Hyperledger Fabric: Architecture, Challenges, and Future Prospects, 11 INT'L J. INNOVATIVE RES. TECH. (2024).

[17] Albina Gaisina & Matthias Finger, *Central Bank Digital Currencies (CBDCs): A Countermeasure to Anti-Money Laundering (AML) Challenges Posed by Cryptocurrencies?,* 7 Digital Finance 201, 230–32 (2025), https://link.springer.com/article/10.1007/s42521-025-00132-9.

[18] Marianne Bechara et al., *Private Law Aspects of Token-Based Central Bank Digital Currencies*, IMF Fintech Note No. 2025/003, at 3–6 (Mar. 2025), https://www.imf.org/-/media/Files/Publications/FTN063/2025/English/FTNEA2025003.ash.

[19] Xu, *supra* note 6.

[20] Raphael A. Auer & Rainer Böhme, *The Technology of Retail Central Bank Digital Currency*, Monetary Economics: Central Banks - Policies & Impacts eJournal (2020).

[21] Bank for International Settlements, *Legal Aspects of Retail CBDCs*, BIS Other Publications No. 88, at 3–5 (Oct. 2023), https://www.bis.org/publ/othp88_legal.pdf.

[22] IndusLaw, *Central Bank Digital Currencies – A Primer on the RBI's Concept Paper*, at 2–4 (Jan. 2022), https://induslaw.com/publications/pdf/alerts-2023/Induslaw-Infolex-Central-Bank-Digital-Currencies.pdf.

[23] Jus Corpus, *Legal Implications of RBI's Digital Rupee: A New Era in Indian Monetary Law*, Jus Corpus Blog (July 6, 2025), https://www.juscorpus.com/legal-implications-of-rbis-digital-rupee-a-new-era-in-indian-monetary-law.

regulations[24]. This places it within the domain of monetary law rather than securities law, aligning it with sovereign currency rather than regulated financial assets.




**Image**: Distinction between wholesale CBDC[25] & Retail CBDC[26] and Five C's[27]

## III. INDIA'S DIGITAL RUPEE: REGULATORY DESIGN AND IMPLEMENTATION

The statutory authority of the Digital Rupee is grounded primarily in Section 22 of the RBI Act[28], 1934, which grants the central bank the exclusive right to issue banknotes. Earlier, the applicability of this provision to digital currency was debated, as the term "banknote" traditionally referred only to physical notes payable to bearer on demand. This ambiguity was explicitly addressed by the Finance Act, 2022[29], which inserted Section 22A[30], empowering the RBI to issue currency "including in digital form", thereby placing the Digital Rupee on the same legal footing as sovereign fiat currency. Consequently, the RBI retains a complete monopoly over CBDC issuance, and commercial banks are restricted to distribution and wallet management functions without any monetary creation authority. The Indian Penal Code provisions on counterfeiting (Sections 489A–489E[31]) have also been interpreted to extend to digital representations of currency, ensuring criminal liability for unauthorized duplication or manipulation of CBDC tokens. Under the Bharatiya Nyay Sanhita, 2023 (BNS), these offenses are now encapsulated under Sections *178 to*

[24] Reserve Bank of India, *Digital Rupee (e₹) – FAQs*, RBI (Jan. 9, 2025), https://www.rbi.org.in/commonperson/english/Scripts/FAQs.aspx?Id=3686.
[25] Chawla, *supra* note 5.
[26] Edwin Ayisi Opare & Kwangjo Kim, *A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures*, 8 IEEE Access 110810 (2020).
[27] Mahesh, *supra* note 10.
[28] Reserve Bank of India Act, 1934, No. 2 of 1934, § 22.
[29] Finance Act, 2022, No. 6 of 2022, § 22A.
[30] Reserve Bank of India Act, 1934, No. 2 of 1934, § 22A.
[31] Indian Penal Code, No. 45 of 1860, §§ 489A–489E.

*181*[32], which criminalize the making, using, circulating, possessing, or facilitating instruments or software intended for counterfeiting "currency or currency in digital form," explicitly recognizing CBDC within the statutory definition of currency. The Payment and Settlement Systems Act, 2007[33], further extends RBI's regulatory control to the entire CBDC infrastructure. Its provisions on authorization, oversight of payment intermediaries, and penalty mechanisms apply directly to entities participating in CBDC distribution and transaction processing. As India moves towards cross-border CBDC trials under BIS mBridge, the Foreign Exchange Management Act, 1999[34], becomes central in determining how Digital Rupee can legally flow across jurisdictions[35]. FEMA[36]'s existing Current and Capital Account rules would govern remittances, speculative CBDC holdings abroad, and the role of authorized dealers in settlement. Parallelly, the Digital Personal Data Protection Act, 2023[37], designates the RBI and participating banks as data fiduciaries, imposing obligations of consent-based processing, data localization of transaction history, and enforceable user rights over access and correction of personal financial data.[38]

Operationally, the Digital Rupee has been deployed through a carefully phased pilot structure. The Wholesale CBDC (e₹-W) was launched on November 1, 2022, initially involving nine major commercial banks[39]. It is currently used for government securities settlement, interbank transactions in the call money market, and is being explored for cross-border wholesale corridors. This wholesale CBDC is integrated into the Clearing Corporation of India Ltd. (CCIL) framework, and as of Q2 2024, over 1,329 wholesale transactions have been executed. The Retail CBDC (e₹-R) pilot began on December 1, 2022, targeting direct public use through wallet-based interfaces managed by 13 authorized banks[40]. With more than 1.3 million users and over 300,000 merchants, the retail pilot supports P2P and P2M payments via QR code infrastructure aligned with UPI standards[41]. A tiered wallet system governs user access, with minimal-KYC basic wallets allowing limited-value pseudonymous transactions, full-KYC standard wallets enabling unrestricted merchant payments, and premium wallets offering offline capability and higher value thresholds.

---

[32] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 178–181.
[33] Payment and Settlement Systems Act, 2007, No. 51 of 2007.
[34] Foreign Exchange Management Act, 1999, No. 42 of 1999.
[35] Xu, *supra* note 6.
[36] *Id.*
[37] Digital Personal Data Protection Act, No. 22 of 2023.
[38] Chawla, *supra* note 5.
[39] Anulekha Ray, *Digital Rupee: RBI Plans to Expand CBDC Pilot to Include More Banks and Locations*, The Economic Times (May 30, 2023), https://economictimes.indiatimes.com/wealth/personal-finance-news/digital-rupee-rbi-to-expand-e-rupee-pilot-to-include-more-banks-and-locations/articleshow/100614794.cms.
[40] Press Information Bureau, *CBDC Pilot Launched by RBI in Retail Segment*, PIB Release (Dec. 12, 2022), https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883.
[41] *India's Digital Rupee Pilot Onboards 1.3 Million Users, 300,000 Merchants*, AInvest (May 22, 2025), https://www.ainvest.com/news/india-digital-rupee-pilot-onboards-1-3-million-users-300-000-merchants-2505.

The integration of CBDC with India's Digital Public Infrastructure (DPI) adds a unique governance dimension to its deployment. The interoperability with UPI ensures that merchant acceptance networks remain unified rather than fragmented, although RBI continues to calibrate measures to prevent CBDC adoption from cannibalizing UPI transaction volumes. Aadhaar-linked eKYC enables instant onboarding, while biometric verification is reserved for high-value transfers in compliance with Supreme Court proportionality tests. The Account Aggregator framework further positions CBDC transaction data as a new layer for credit scoring and financial inclusion, especially for MSME and rural lending ecosystems. Complementary DPI layers like GSTN, Co-WIN, and ONDC present potential integration points for programmable CBDC payments, automated tax compliance, and public benefit transfers[42].

To support innovation, the RBI Innovation Hub operates as a regulatory sandbox for testing programmable transactions, offline settlement designs, and cross-border CBDC interoperability. The Public Tech Platform for Frictionless Credit explores how CBDC transaction trails can aid in real-time credit assessment, especially for agriculture finance through Kisan Credit Card digitization. BBPS integration allows recurring bill payments using Digital Rupee, advancing RBI's objective of reducing cash friction in semi-urban and rural economies[43]. Financial inclusion remains a core mandate, with targeted initiatives such as training Business Correspondents, deploying regional language CBDC apps[44], and subsidizing smartphone access for Jan Dhan households to achieve a projected 500 million CBDC-ready citizens by 2027[45].

Despite its strong statutory backing and phased rollout, the CBDC ecosystem faces regulatory challenges that demand precise legal responsiveness. The risk of double-spending and cyber fraud is directly tied to the digital nature of CBDC and is mitigated through cryptographic validation and unique serial identification of tokens. Offline transaction capability introduces an additional risk layer, as real-time reconciliation is not always possible; hence RBI has adopted a hybrid settlement protocol with capped offline limits. CBDC must also align with FATF and PMLA guidelines on KYC/AML enforcement without excluding low-income or undocumented populations from financial access, which is being addressed through tiered KYC frameworks[46]. Under the DPDP Act[47], transaction history becomes protected personal data, raising new compliance questions around purpose limitation and data minimization, especially when CBDC data is considered for

[42] Mahrous, *supra* note 2.
[43] Public Tech Platform for Frictionless Credit, PTPFC, https://ptpfc.org.
[44] K. M. Mahesh et al., *Impact of Centralized Blockchain Digital Currency (CBDC): For Financial Inclusion and Sustainability*, International Journal of Management, Technology, and Social Sciences (2024).
[45] Reserve Bank of India, *RBI to Launch Pilot Project for Public Tech Platform for Frictionless Credit*, Press Release (Aug. 14, 2023), https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=56200 .
[46] Auer, *supra* note 20.
[47] Digital Personal Data Protection Act, No. 22 of 2023.

credit analytics or behavioral profiling[48]. There are also concerns about potential bank disintermediation, where large-scale migration of deposits to CBDC wallets could deprive commercial banks of lending capital. RBI currently mitigates this risk by maintaining non-interest-bearing CBDC design, exploring balance caps, and retaining parallel infrastructure for bank deposits and physical cash. Finally, legal certainty is required on claim enforceability in cases where a payment service provider managing a CBDC wallet becomes insolvent. Ensuring segregation of user balances and portability of wallets across intermediaries may necessitate new statutory provisions similar to deposit insurance frameworks, bringing CBDC regulation closer to the robustness of traditional banking law.

## IV. COMPARATIVE ANALYSIS: GLOBAL CBDC MODELS

While China's e-CNY enforcement framework relies heavily on administrative mandates and real-time cybersecurity supervision to deter unauthorized manipulation of digital tokens, India has opted for a more formal statutory route through the *Bharatiya Nyay Sanhita (BNS), 2023*, which replaces the Indian Penal Code. The former IPC provisions on currency counterfeiting (Sections 489A–489E[49]) have been systematically recast into Sections 178–181 of the BNS[50], with a significant doctrinal expansion the definition of "currency" now explicitly includes "currency in digital form", bringing CBDC-related offenses squarely within the ambit of criminal prosecution. Under Section 179 of the BNS[51], not only the physical circulation of counterfeit notes but also the transfer of fake CBDC tokens such as QR-based payments using manipulated e₹ units, constitutes a punishable offense. Likewise, Section 181[52] extends the offence of possessing instruments for counterfeiting to include software scripts, malicious code, and unauthorized cryptographic tools designed to duplicate or simulate CBDC wallet balances[53]. This represents a marked departure from frameworks like the EU, which place greater emphasis on regulatory compliance and data governance rather than punitive criminal enforcement.

Further, digital impersonation via fake CBDC wallets, Aadhaar-spoofed KYC, or UPI-linked identity fraud is now categorized as "cheating by personation using electronic means" under Section 316 of the BNS[54], replacing the IPC 419 + IT Act 66C regime. The Bharatiya Sakshya Adhiniyam, 2023[55] modernizes evidentiary standards by recognizing CBDC ledger entries, UPI

[48] Vučinić, *supra* note 12.
[49] Xu, *supra* note 6.
[50] *Id.*
[51] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 179.
[52] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 181.
[53] Vučinić, *supra* note 12.
[54] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 31.
[55] Bharatiya Sakshya Adhiniyam, No. 47 of 2023.

transaction logs, and RBI wallet metadata as primary electronic evidence, eliminating the procedural hurdles previously associated with Section 65B certification under the Evidence Act[56]. The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023[57] further consolidates the enforcement ecosystem by classifying unauthorized access to CBDC systems or manipulation of wallet infrastructure as cognizable offenses, enabling law enforcement to arrest without warrant in high-value digital currency fraud cases. This gives India a centralized, statute-backed enforcement model, in contrast to the United States, where CBDC does not yet exist and enforcement would be fragmented across multiple federal and state authorities[58].

Overall, India's legal posture positions it uniquely within the CBDC landscape, combining a sovereign-issued digital currency with a purpose-built criminal law framework that directly targets duplication, manipulation, and unauthorized circulation of digital legal tender. This creates a jurisprudentially robust foundation that aligns with emerging multilateral platforms like BIS Project mBridge[59], where effective cross-border CBDC settlement requires clear domestic criminal liability regimes.

While India has codified a CBDC-specific criminal liability regime, China does not create a separate penal category for e-CNY misuse. Instead, it subsumes all illicit digital currency activity under existing RMB counterfeiting provisions in the *Penal Law (Articles 170–174[60])*, bolstered by expansive administrative enforcement powers under the *PBOC Law*[61] and Cybersecurity Law[62]. Enforcement is technologically embedded, allowing pre-trial wallet freezing and device blocking by Public Security Bureaus without resort to judicial process, under the doctrine of "controllable anonymity."[63][64]

In contrast, the European Union adopts a data rights and procedural fairness model. Misuse of the digital euro would not automatically be treated as currency counterfeiting; instead, it would fall under Directive (EU) 2019/713[65] on fraud involving non-cash means of payment, interpreted alongside GDPR and eIDAS. Here, CBDC violations are framed as payment system abuse and

[56] Indian Evidence Act, 1872, No. 1 of 1872, § 65B.
[57] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023.
[58] Opare, *supra* note 26.
[59] Chawla, *supra* note 5.
[60] Criminal Law of the People's Republic of China, arts. 170–174, Order No. 83, Mar. 14, 1997, amended Dec. 26, 2020, Standing Comm. Nat'l People's Cong. (P.R.C.), https://en.spp.gov.cn.
[61] Law of the People's Republic of China on the People's Bank of China, Order No. 46, Mar. 18, 1995, amended Dec. 27, 2003, Standing Comm. Nat'l People's Cong. (P.R.C.), http://www.pbc.gov.cn..
[62] Cybersecurity Law of the People's Republic of China, Order No. 53, Nov. 7, 2016, effective June 1, 2017, Standing Comm. Nat'l People's Cong. (P.R.C.), Stanford Digi China Translation.
[63] Xu, *supra* note 6.
[64] Mahesh, *supra* note 44.
[65] Directive (EU) 2019/713, of the European Parliament and of the Council, Apr. 17, 2019, on combating fraud and counterfeiting of non-cash means of payment, 2019 O.J. (L 123) 18 (EU), https://eur-lex.europa.eu/eli/dir/2019/713/oj.

data integrity breaches, placing privacy and proportionality above sovereign enforcement imperatives.

The United States, lacking a CBDC, operates on a projected enforcement logic. Any future digital dollar misuse would likely be prosecuted under existing financial crime statutes, 18 U.S.C. §§471–474[66] (counterfeiting), §1028A[67] (identity theft), §1343[68] (wire fraud), and the Computer Fraud and Abuse Act[69] (CFAA), with enforcement divided between the FBI and Secret Service. However, widespread political resistance to a CBDC on grounds of "financial surveillance" suggests that any attempt to classify CBDC token tampering as a sovereign currency offence would face robust Fourth Amendment scrutiny.

## V. CROSS-BORDER PAYMENT IMPLICATIONS AND JURISDICTIONAL CHALLENGES

The current architecture of cross-border payments, dominated by the correspondent banking model, suffers from inherent inefficiencies that disproportionately impact high-remittance economies like India. Traditional remittance channels impose a multi-layered cost structure; global World Bank data for 2023 places the average remittance cost at 6.2% per transaction, compounded by intermediary correspondent bank fees ranging between 1–3% and foreign exchange spreads of 2–5%.[70] For India, which receives over $100 billion in annual inward remittances, this translates into an economic leakage exceeding $6 billion in transaction costs alone[71]. These financial burdens are exacerbated by systemic time delays, with settlement cycles ranging from 3–5 working days and extending beyond a week for transactions routed through less liquid currency corridors. Cut-off times, weekend closures, and sequential compliance checks across multiple jurisdictions further slow down processing.

Beyond cost and speed, opacity remains a defining flaw of the SWIFT-based correspondent model. Transaction routing across multiple intermediary banks introduces duplicative Know-Your-Customer (KYC) and Anti-Money Laundering (AML) checks, fragmented sanctions screening, and limited visibility for end-users tracking payments in real time. Such friction is compounded by the trend of global "de-risking," wherein major correspondent banks withdraw from jurisdictions perceived as high-risk, reducing available corridors and increasing reliance on limited channels with

[66] 18 U.S.C. §§ 471–474 (2023).
[67] 18 U.S.C. § 1028A (2023).
[68] 18 U.S.C. § 1343 (2023).
[69] 18 U.S.C. § 1030 (2023).
[70] World Bank, *Remittance Prices Worldwide – Issue 47*, at 3 (Sept. 2023), https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q423_final.pdf.
[71] Press Information Bureau, *Annual Remittances to India Reach $125 Billion*, PIB Release (Dec. 19, 2023), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2023/dec/doc20231219290501.pdf.

higher cost structures. For India, this introduces vulnerability, particularly with respect to the Gulf region, its single-largest remittance source, where banking de-risking could jeopardize financial inclusion for overseas workers.

In this context, Central Bank Digital Currencies (CBDCs) emerge as a structural alternative to legacy correspondent banking. Wholesale CBDC models introduce three plausible architectures for cross-border settlements. The first is a bilateral CBDC bridge model, wherein two central banks establish a direct digital settlement corridor with atomic cross-ledger swaps, preserving monetary sovereignty while enabling near-instant settlements. A potential RBI-Monetary Authority of Singapore (MAS) INR-SGD[72] wholesale corridor exemplifies this approach. The second, more advanced design is the multi-CBDC shared ledger model, represented by the BIS-led mBridge initiative[73], where multiple central banks issue and transact their CBDCs over a common technical infrastructure using smart contracts for automated conversion and settlement. This model offers superior interoperability and network effects but raises complex questions around shared governance and jurisdictional authority. The third model relies on interlinking domestic CBDCs through FX platforms, integrating private intermediaries like CLS to facilitate currency conversion without merging sovereign infrastructures, thereby maximizing autonomy but reintroducing intermediary risk elements.

Retail CBDC cross-border use cases introduce further possibilities.[74] Under a tourist and remittance wallet model, foreign users may temporarily hold limited-purpose e₹ balances after simplified onboarding through passport-based KYC, similar to China's e-CNY deployment during the 2022 Winter Olympics[75]. Alternatively, a wallet interoperability model could allow domestic apps to host foreign CBDCs with real-time FX conversion, contingent on deep technical and legal harmonization between participating central banks. For high-volume corridors like India-UAE, a CBDC remittance corridor architecture could facilitate instant, low-cost transfers with shared AML/CFT compliance responsibilities between the RBI and the Central Bank of the UAE, positioning CBDCs as a direct policy instrument for remittance cost reduction[76].

---

[72] The Hindu, *RBI Explores Cross-Border CBDC Pilots as e₹ Circulation Surges* (May 29, 2025), https://www.thehindu.com/business/e-rupee-in-circulation-grows-to-1016-crore-rbi-explores-cross-border-cbdc-pilots/article69632789.ece.

[73] Forbes, *Cross-Border CBDC Focused Project mBridge Moves Forward* (June 23, 2024), https://www.forbes.com/sites/digital-assets/2024/06/23/cross-border-cbdc-focused-project-mbridge-moves-forward.

[74] Auer, *supra* note 20.

[75] Xu, *supra* note 6.

[76] Mahesh, *supra* note 44.

However, these innovations trigger complex jurisdictional and legal challenges. Under Indian FEMA regulations[77] fundamental ambiguities arise regarding whether a domestic resident holding e₹ abroad constitutes a current or capital account transaction and whether FEMA's currency holding caps extend to CBDC wallets. Similarly, when a foreign national holds Digital Rupee, the legal tender status becomes territorially ambiguous, raising questions on enforceability and tax obligations. In a multi-CBDC environment like mBridge, determining the applicable legal system for dispute resolution, particularly when smart contracts autonomously execute cross-currency swaps presents an unresolved conflict-of-laws dilemma. These issues necessitate statutory clarification, particularly through amendments to FEMA[78] defining CBDCs as a distinct legal category separate from conventional foreign exchange assets.

Furthermore, AML compliance under FATF's "travel rule" requires reconciling the pseudonymity of token-based CBDC systems with mandatory identity disclosures in cross-border transactions[79]. Indian legal obligations under the Prevention of Money Laundering Act (PMLA), such as Section 12 (record keeping) and Section 12A[80] (client due diligence), need calibrated integration into CBDC protocols[81] through tiered anonymity models, where domestic low-value transactions remain private, while cross-border transfers trigger identity-linked reporting mechanisms and real-time suspicious transaction alerts via bilateral FIU integration.

Taxation and transfer pricing concerns further complicate CBDC deployment in international settlements. Under Section 195 of the Income Tax Act[82], withholding tax obligations apply to payments made to non-residents, but CBDC-based pseudonymous transactions may obscure payer identity unless explicit compliance triggers are embedded at protocol level. GST applicability on digital services paid via e₹ would depend on "place of supply" rules, demanding CBDC-specific interpretive guidance. For multinational corporations using CBDCs for intra-group settlements, transfer pricing compliance would necessitate transparent CBDC transaction documentation and potentially new Advance Pricing Agreement (APA) frameworks adapted to CBDC corridors[83].

At the macroeconomic level, India faces a monetary sovereignty trilemma. Full sovereignty over e₹ issuance, seamless cross-border CBDC interoperability, and absolute financial stability cannot

[77] Foreign Exchange Management (Overseas Investment) Regulations, No. FEMA 400/2022-RB, Gazette of India, Aug. 22, 2022.
[78] Chawla, *supra* note 5.
[79] Financial Action Task Force, *FATF Updates Standards on Recommendation 16 on Payment Transparency*, FATF (June 18, 2025), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html.
[80] Prevention of Money Laundering Act, No. 15 of 2003, §§ 12–12A (India), amended by Act No. 2 of 2013.
[81] Bank for International Settlements, *Project mBridge: Building a Multi-CBDC Platform for International Payments*, Sept. 2022, https://www.bis.org/publ/bppdf/bispap125.pdf.
[82] Income-tax Act, No. 43 of 1961, § 195.
[83] Mahrous, *supra* note 2.

be simultaneously achieved. India's current strategy prioritizes sovereignty through controlled issuance and restrictive FEMA-led capital controls, while cautiously experimenting with selective bilateral corridors, reflecting a phased interoperability approach[84]. Fragmentation risks persist, however, as divergent CBDC standards could lead to regional digital currency blocs unless harmonized under BIS, IMF, or G20-led governance frameworks[85].

Strategically, India views the Digital Rupee as a geopolitical instrument for rupee internationalization, enabling CBDC-based trade invoicing for energy imports and BRICS-led de-dollarization initiatives. In the remittance domain, integrating e₹ corridors with key jurisdictions like UAE and Singapore offers the potential to reduce transaction costs by up to 90%. Multilaterally, platforms like BRICS Pay and ASEAN's Project Nexus[86] offer fertile ground for Digital Rupee integration, building on existing UPI-PayNow linkages and expanding them into a CBDC settlement layer.[87]

Stablecoins have demonstrated utility in cross-border payments, remittances, and trade finance. However, they also expose jurisdictional vulnerabilities, AML/CFT compliance, taxation, and exchange control. The Digital Rupee's cross-border phase must contend with FEMA restrictions[88] and international standards such as ISO 20022.[89]

The survey paper identifies regulatory arbitrage and extraterritoriality as key risks. Without harmonized legal frameworks, CBDCs may replicate the fragmentation seen in stablecoin markets. India's leadership in BRICS Pay and ASEAN linkages offers a strategic opportunity to shape South-South CBDC cooperation.[90]

## VI. DATA, PRIVACY, AND SOVEREIGNTY IN THE CBDC REGIME

The introduction of CBDCs globally has reignited the classical tension between monetary surveillance and individual financial privacy. CBDCs, by design, create a digital trace for every unit of currency, unlike physical cash which leaves no transactional footprint. This produces what may be termed the surveillance, anonymity dilemma, within which jurisdictions are experimenting with varied privacy models along a spectrum ranging from full anonymity to complete traceability. A cash-like anonymity model, involving zero identity disclosure and unrestricted peer-to-peer

[84] Vučinić, *supra* note 12.
[85] Chawla, *supra* note 5.
[86] Reserve Bank of India, *RBI and ASEAN Countries to Create a Platform to Facilitate Instantaneous Cross-Border Retail Payments,* Press Release, Jul. 1, 2024, https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=58197.
[87] Opare, *supra* note 26.
[88] Foreign Exchange Management (Overseas Investment) Regulations, 2022, No. FEMA 400/2022-RB, Gazette of India, Aug. 22, 2022.
[89] Committee on Payments and Market Infrastructures, *Harmonised ISO 20022 Data Requirements for Enhancing Cross-Border Payments*, Bank for Int'l Settlements, Oct. 17, 2023, https://www.bis.org/cpmi/publ/d218.htm.
[90] Mahrous, *supra* note 2.

transfers beyond the view of intermediaries or the state, has been conceptually discussed but rejected by all major central banks due to its potential to facilitate illicit finance, tax evasion, and sanctions circumvention[91]. In contrast, the pseudonymous tiered model, which India has adopted, allows limited identity disclosure for low-value CBDC wallets while mandating full KYC compliance and transaction traceability for higher-value transfers, thus retaining investigatory visibility for law enforcement under due process. At the other end of the spectrum lies the full traceability model, exemplified by China's e-CNY, where every transaction is identity-linked and centrally monitored in real time under the doctrine of "controllable anonymity."

In India's constitutional context, such levels of surveillance necessarily invite scrutiny under the fundamental right to privacy articulated in *Justice K.S. Puttaswamy v. Union of India,*[92] which held that informational privacy, including financial data, falls within the protection of Article 21[93]. Any intrusion by the state into personal transaction data must therefore satisfy the tripartite test of legality, legitimate state aim, and proportionality. While combating money laundering, ensuring tax compliance, and preserving monetary stability are arguably legitimate aims, a question arises as to whether a fully traceable CBDC architecture would be a proportionate restriction or whether a tiered privacy approach, like the one currently adopted by the RBI, better aligns with constitutional standards. Litigation may emerge if CBDC regulations were to mandate identity linkage for all categories of users or impose excessive data disclosure obligations without strong procedural safeguards.

This debate directly intersects with India's evolving data protection regime under the Digital Personal Data Protection Act (DPDP), 2023[94], which treats the RBI and participating banks as Data Fiduciaries responsible for lawful processing and protection of CBDC transaction data, while payment intermediaries function as Data Processors operating under delegated compliance.[95] The DPDP Act[96] imposes principles of purpose limitation, data minimization, storage limitation, and security safeguards, meaning that CBDC-related data collection must be strictly limited to what is necessary for payment settlement, AML obligations, or monetary policy functions. However, potential conflicts arise between the data minimization mandate and reporting requirements under

[91] ICAIE, *Central Bank Digital Currencies: Risks and Rewards – Global Finance and the Fight Against Money Laundering*, ICAIE Report (Jan. 7, 2025), https://icaie.com/2025/01/icaie-releases-new-report-on-central-bank-digital-currencies-risks-and-rewards-global-finance-and-the-fight-against-money-laundering.
[92] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
[93] India Consti. Art. 21.
[94] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 179.
[95] Vučinić, *supra* note 12.
[96] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 179.

PMLA[97] and FATF standards[98], which require exhaustive transaction monitoring. The DPDP Act[99] provides an exemption for legal obligations, but ambiguity persists regarding whether economic analysis, behavioral profiling, or credit-scoring based on CBDC data falls within the RBI's statutory mandate or constitutes excessive data use requiring explicit user consent.[100]

A comparative glance at global CBDC models reveals three distinct privacy governance orientations. China's e-CNY adopts a state-surveillance-first approach, allowing only minimal pseudonymity while ensuring full visibility for the central bank, with transactional metadata such as device ID, IP address, and location logs retained indefinitely. Such a system aligns with China's broader cybersecurity and data localization regime, where state access eclipses individual data rights[101]. In contrast, the European Union's Digital Euro project adopts a privacy-by-design architecture, mandating GDPR-compliant data minimization, anonymized offline transactions, and the use of cryptographic techniques like zero-knowledge proofs to verify compliance without revealing user identity or spending patterns[102]. India occupies an intermediate position, adopting a tiered compromise model under which basic low-value wallets retain some pseudonymity to support inclusion and microtransactions, while higher-value usage triggers stricter KYC thresholds and deeper supervisory visibility.

As India enters cross-border CBDC experiments such as Project mBridge, the issue of data sovereignty becomes even more pressing. The RBI's 2018 data localization mandate[103] requires all payment-related data to be stored exclusively on Indian servers, with only limited, regulated data mirroring permitted abroad. However, cross-border CBDC platforms operate on shared ledgers distributed across multiple jurisdictions, raising the risk that Indian CBDC transaction data could be stored on foreign nodes and subjected to foreign data access laws such as the US CLOUD Act or China's National Intelligence Law, both of which compel companies to disclose data to national authorities regardless of where it is stored. To prevent extraterritorial surveillance, India would need to enforce technical safeguards like domestic-only data residency, encryption with sovereign key control, and legal clauses within bilateral CBDC arrangements prohibiting foreign data claims. Additionally, any interoperation with European CBDC systems will trigger GDPR adequacy requirements, for which India's DPDP framework currently falls short due to the absence of an

[97] Prevention of Money Laundering Act, No. 15 of 2003.
[98] Financial Action Task Force (FATF), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (updated June 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.
[99] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 179.
[100] Opare, *supra* note 26.
[101] Xu, *supra* note 6.
[102] Mahrous, *supra* note 2.
[103] Reserve Bank of India, *Storage of Payment System Data*, Circular No. DPSS.CO.OD.No 2785/06.08.005/2017-18, Apr. 6, 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

independent data protection authority with strong enforcement powers. Strengthening domestic data governance institutions will therefore be a prerequisite for India to assert true data sovereignty in cross-border CBDC use[104].

## VII. LEGAL REFORM AND POLICY RECOMMENDATIONS

A coherent CBDC ecosystem cannot rest solely on pilot experimentation and regulatory circulars; it requires statutory precision and legislative architecture that clearly defines the legal status, enforceability, liability regime, and cross-border operability of digital currency. To that end, amendments to India's financial legal framework must be both targeted and future-proof, calibrated to preserve monetary sovereignty while enabling technologically adaptive governance. The insertion of a new Section 22A into the RBI Act, 1934[105], explicitly recognizing the RBI's authority to issue digital currency with full legal tender status, would eliminate interpretive ambiguity around whether e₹ constitutes "currency" or merely a regulated payment instrument. Supplementary amendments to Sections 31 and 58 would not only mandate 100% reserve backing for intermediaries managing CBDC wallets, preventing fractionalization of sovereign digital currency but also criminalize unauthorized issuance or counterfeiting, aligning digital monetary protection with the severity traditionally accorded to physical currency integrity.[106]

Complementing the RBI Act[107], the Payment and Settlement Systems Act, 2007, requires definitional expansion to incorporate CBDC as a distinct payment category, accompanied by a new Section 4A establishing authorization, interoperability and dispute resolution standards specific to CBDC infrastructure. Parallel to this, amendments to FEMA, 1999, through a dedicated Section 3A on cross-border CBDC flows, are essential to govern the holding, transfer and conversion of foreign digital currencies within India's capital control regime, ensuring that digitization does not create a regulatory backdoor for uncontrolled foreign currency circulation. Critically, the Digital Personal Data Protection Act, 2023, must be refined to embed CBDC transaction data within a regulated exception framework, permitting controlled processing for monetary stability and AML purposes while prohibiting commercial exploitation or non-regulatory profiling. A new Section 18A under DPDP[108] would institutionalize user rights to access, rectification and transparency in CBDC data handling, anchoring financial privacy as a statutory entitlement rather than a discretionary administrative assurance.[109]

---

[104] Auer, *supra* note 20.
[105] Cole, *supra* note 3.
[106] Chawla, *supra* note 5.
[107] Cole, *supra* note 3.
[108] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 179.
[109] Mahesh, *supra* note 44.

Beyond legislative text, regulatory refinement through a dedicated RBI Master Direction on CBDC would operationalize supervisory expectations across technological standards, intermediary licensing, consumer redressal and cross-border compliance.[110] Such a framework must articulate offline transaction protocols, wallet portability rights, zero-liability norms for unauthorized digital rupee transactions and tiered KYC systems aligned with FATF guidelines. Interoperability sits at the core of CBDC functionality; therefore, the adoption of ISO 20022 messaging formats, UPI-compatible QR logic, open APIs and offline connectivity frameworks (NFC/Bluetooth mesh protocols) becomes essential to prevent CBDC from becoming a parallel, isolated payment system rather than an integrated layer of India's digital financial infrastructure[111]. Legal interoperability, too, demands attention, standardized choice-of-law clauses, CBDC arbitration templates and mutual recognition agreements must accompany technical integration to ensure cross-border legal enforceability.

To give CBDC geopolitical and trade relevance, India must transition from pilot-stage diplomacy to treaty-grade monetary coordination, beginning with bilateral digital currency agreements with high-volume corridors such as the UAE, Singapore, UK and Saudi Arabia. These agreements should not merely provide transactional permissions but establish a comprehensive governance framework, specifying settlement architecture, recognition of KYC identities, AML data-sharing protocols, dispute resolution through BIS-linked arbitration, and explicit exit clauses to protect user holdings in scenarios of diplomatic breakdown or technical severance. India's evolving participation in Project mBridge offers a strategic foothold to embed the rupee in multilateral CBDC clearing pathways. By upgrading from observer to full participant with node infrastructure hosted in Mumbai, India can influence governance rules, technical standards and onboarding criteria for future participant economies, ensuring that global CBDC frameworks do not default to yuan or dollar dominance.

In parallel, BRICS-level CBDC cooperation presents an opportunity to design a South-led digital financial bloc, with the Digital Rupee positioned as one of multiple interoperable CBDCs within a non-dollar settlement ecosystem. This vision would be further amplified by embedding CBDC transaction support within New Development Bank financing and BRICS Pay architectures, reducing dependence on Western-controlled correspondent banking channels[112]. Leveraging its demonstrable success with digital public infrastructure and its normative advantage as a democratic technology state, India is uniquely positioned to lead a Global South CBDC Knowledge and Legal Harmonization Network. Such an initiative, featuring an open-source CBDC stack modelled on

[110] Vučinić, *supra* note 12.
[111] Mahesh, *supra* note 44.
[112] Mahrous, *supra* note 2.

India Stack, model legislation for developing central banks and technical training programs would not only institutionalize India's leadership but also construct an alternative to Western regulatory dominance in digital currency governance.

## VIII. CONCLUSION

India's Digital Rupee represents a cautiously ambitious experiment at the intersection of monetary policy, financial technology and legal innovation. Anchored in statutory legitimacy and layered upon a decade of digital public infrastructure, the e₹ stands out as a pragmatic model for emerging economies seeking to reconcile innovation with regulatory prudence, financial inclusion with compliance imperatives, and domestic sovereignty with the realities of global economic interdependence. By selecting a hybrid architecture, centralized issuance by the RBI with intermediated distribution through commercial banks, India has avoided both extremes: neither the state-monopoly design of China's e-CNY, nor the multi-sovereign coordination difficulties faced by the European Union. This architectural pragmatism enhances scalability while preserving the RBI's monetary authority and leveraging existing banking networks for consumer interface and risk management.

Yet, the legal foundations, while grounded in the RBI Act, PSSA, and FEMA remain incomplete. Without a dedicated CBDC statute, questions persist on the enforceability of digital rupee contracts, cross-border settlements, consumer liability in failed transactions, and the legal status of programmability features. These structural ambiguities could generate friction as adoption scales and cross-border corridors emerge. Privacy emerges as a persistent site of constitutional negotiation: India's tiered anonymity model reflects an attempt to reconcile low-barrier financial inclusion, AML/CFT compliance, and the right to informational privacy under Article 21. The durability of this compromise will depend on strict implementation of the Digital Personal Data Protection Act, 2023, credible supervisory oversight, and judicial readiness to enforce the privacy-proportionality doctrine laid down in Puttaswamy.

Cross-border use of CBDCs offers both strategic promise and systemic risk. Through participation in mBridge and potential bilateral corridors with the UAE, Singapore and the UK, the Digital Rupee could reduce remittance frictions, enhance rupee settlement in trade flows and diversify India's financial linkages in a fragmenting global economy. However, data sovereignty, jurisdictional conflicts under FEMA, and the absence of harmonized global legal norms for CBDCs risk the creation of fragmented currency blocs rather than a coherent interoperable system. This reflects a broader shift toward "fragmented globalization," where CBDCs become instruments of geopolitical alignment as much as financial innovation.

This moment carries consequences beyond technology. CBDCs signify a renewed assertion of monetary sovereignty by central banks after a decade in which private cryptocurrencies and stablecoins challenged the state's monopoly over currency issuance. At the same time, in economies like India and China, CBDCs will shape global norms around financial surveillance. If CBDCs are perceived as surveillance tools rather than instruments of inclusion, public trust may erode, turning a monetary innovation into a site of civil resistance. India's success, therefore, depends not just on technological rollout, but on the credibility of its legal safeguards, transparency protocols and democratic accountability mechanisms.

Looking forward, the evolution of CBDCs will hinge on what can be described as "collaborative sovereignty", a model where domestic monetary control is preserved, but international interoperability, shared technical standards and rights-based governance frameworks allow seamless, rights-respecting cross-border payments. For India, achieving this vision requires domestic legal consolidation, international treaty negotiation and technological leadership. A mature CBDC ecosystem by 2030 would require: (1) statutory clarity through legislative amendments and a dedicated CBDC Act; (2) institutional strengthening of data protection enforcement with independent oversight; (3) scale expansion to a critical mass of over 100 million active users; (4) operational cross-border corridors with at least 10 major trading partners, and (5) a visible role in BIS, IMF and BRICS-led standard-setting forums to shape norms rather than merely adapt to them.

Ultimately, the Digital Rupee experiment is not just about engineering a new payment rail. It is a constitutional, economic and geopolitical project, positioned at the fault lines of state power, individual rights and global financial governance. As India advances, its design choices on privacy, legal enforceability, data sovereignty and interoperability will influence global digital currency architectures for decades to come. The digital currency moment is here; whether it leads to empowerment or enclosure will depend on how nations like India navigate the tension between control and openness, innovation and ethics, sovereignty and cooperation.[113]

[113] *Id.*

*This page is intentionally left blank*

Adv. K Gopika & Adv. K Devika, *The DPDP Act and Kerala Bank: A Case Study Iin Data Governance and Risk Management,* 12 (1) SCHOLASTICUS 1 (2025)

# THE DPDP ACT AND KERALA BANK: A CASE STUDY IN DATA GOVERNANCE AND RISK MANAGEMENT

*Adv. K Gopika[*] & Adv. K Devika[†]*

*ABSTRACT*

*India's approach to data governance and privacy has undergone a major shift with the passage of the Digital Personal Data Protection Act, 2023. It aims to create a uniform framework for the public and private sectors to handle, maintain, and safeguard personal data This new regime presents significant compliance challenges for the banking industry, one of the biggest processors of sensitive financial and personal data. As a state-regulated cooperative bank, Kerala Bank offers a unique example of how regional banks adjust to their responsibilities regarding data security and cyber governance. This paper evaluates how the DPDP Act impacts Kerala Bank's data governance framework, focusing on ability to operate, customer trust, and institutional risk management. It also looks at how the Act affects governance structures, capacity building, and compliance architecture in cooperative banking systems. The study also explores how Kerala Bank can improve its cyber security, transparency, and long-term depositor trust by utilizing the DPDP Act. By demonstrating that privacy protection is not only a legal necessity but also a fundamental component of sustainable banking governance in India, this study ultimately seeks to close the gap between legal compliance and real-world implementation.*

[*] Adv. K Gopika is a LL.M student at Central University of Kerala, and can be contacted at advgopikaprabha20601[at]gmail[dot]com

[†] Adv. K. Devika is a LL.M student at Central University of Kerala, and can be contacted at devikaprabha14[at]gmail[dot]com

## I. INTRODUCTION

India's financial system has rapidly gone digital over the past ten years. Technology-driven services like digital payment gateways, mobile applications, online banking, and Aadhaar-based authentication systems have become more and more important to banks.[1] These developments have increased efficiency and accessibility, but they have also put financial institutions at serious risk from cyber fraud, illegal access, and data misuse.[2] In order to address these growing concerns, a comprehensive framework for protecting personal data was introduced by the Digital Personal Data Protection Act, 2023 (DPDP Act).[3] In the banking system, where sensitive personal and financial data is continuously processed, the Act places a strong emphasis on the principles of consent, purpose limitation, data minimization, and accountability.[4]

## II. EVOLUTION OF DATA PROTECTION IN INDIA

India lacked a specific law protecting personal data prior to the DPDP Act. A combined set of provisions under the Information Technology Act, 2000 (IT Act) and its implementing regulations addressed data privacy concerns.[5] These clauses, however, came inadequate in addressing the contemporary issues brought about by global data sharing, financial technology innovation, and digital platforms.[6] According to Article 21 of the Constitution, privacy was acknowledged as a fundamental right in the 2017 ruling in *Puttaswamy v. Union of India*.[7] The DPDP Act was eventually passed in 2023 as a result of this historic decision, which set the groundwork for a new privacy law.[8] Despite being modified to fit India's socioeconomic circumstances, the Act complies with international standards such as the[9] EU's General Data Protection Regulation (GDPR).[10]

## III. THE BANKING SECTOR AND DATA GOVERNANCE

Banks manage huge quantities of personal data, such as financial credentials, transaction histories, and biometric identifiers. According to the DPDP Act, they are therefore considered high-risk processors.[11] Numerous circulars on cybersecurity, data localization, and consumer consent in digital transactions have already been released by the Reserve Bank of India (RBI).[12] Nevertheless,

---

[1] Ministry of Electronics & IT, "Digital India Programme Overview" (2022).
[2] CERT-In, Annual Cybersecurity Report (2022).
[3] DPDP Act, § 3.
[4] Justice B.N. Srikrishna Committee Report on Data Protection (2018).
[5] Information Technology Act, No. 21 of 2000, § 43A.
[6] Internet Freedom Foundation, "Why India Needed a New Data Law" (2023).
[7] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[8] DPDP Bill, Lok Sabha Debates, Aug. 2023.
[9] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[10] *Id.* § 4.
[11] RBI Circular on Cyber Security Framework in Banks (June 2, 2016).
[12] *Id.* § 7-10.

the DPDP Act adds new responsibilities like: Getting customers' express consent for data use, Ensuring fair and legal data processing, establishing procedures for data correction and grievance redress notifying the Indian Data Protection Board of data breaches. Due to limited infrastructure, technological limitations, and resource availability, these requirements present operational challenges for cooperative banks such as Kerala Bank.[13]

## IV. KERALA BANK: A UNIQUE INSTITUTIONAL FRAMEWORK

In 2019, a number of Kerala district cooperative banks merged to form Kerala Bank, also referred to as the Kerala State Co-operative Bank.[14] The RBI and the Kerala State Co-operative Societies Act, 1969 both regulate its operations.[15] Compared to commercial banks, compliance is more complicated because of this dual nature. Millions of customers' personal data is handled by Kerala Bank as it grows its online presence by providing internet services, mobile banking, and Aadhaar-based financial inclusion initiatives, especially in rural and semi-urban areas.[16]Therefore, DPDP compliance mechanism implementation becomes both a legal requirement and a means of enhancing public confidence in the cooperative banking system.[17]

## V. OVERVIEW OF THE DPDP ACT AND ITS RELEVANCE TO THE BANKING SECTOR

A significant legal turning point in India's continuous efforts to guarantee better protection of digital privacy and data rights was the Digital Personal Data Protection Act, 2023, also referred to as the DPDP Act. The Supreme Court's historic ruling in Justice *K.S. Puttaswamy v. Union of India (2017)*, which maintained that privacy is a fundamental right under Article 21 of the Indian Constitution, caused years of policy debate before the law was passed.[18] The government can now draft a comprehensive law that regulates the collection, processing, storage, and sharing of personal data due to the constitutional foundation established by that ruling. . The Justice B.N. Srikrishna Committee was formed by the Indian government in response to this court order, and it produced a thorough report in 2018 suggesting a contemporary data protection framework. Its fundamental principle was that people must maintain control over their personal data, even though digital innovation is essential for economic growth.[19] Enacted in 2023, the DPDP Act aims to achieve

[13] Kerala Cooperative Banking Federation Policy Note (2022).
[14] Government of Kerala, Notification on Formation of Kerala Bank, 2019.
[15] Kerala State Cooperative Societies Act, 1969, § 74A.
[16] Kerala Bank Annual Report (2023).
[17] RBI Financial Stability Report (2023).
[18] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[19] Justice B.N. Srikrishna Committee Report on Data Protection (2018).

balance between advancing India's digital economy and guaranteeing that citizens' privacy is protected throughout the entire data processing process. The Act aims to protect the rights of individuals, known as "Data Principals," and to impose duties on organizations that gather and utilize data, known as "Data Fiduciaries." [20] In short, the law seeks to create a setting where individuals are aware of what happens to their data and where organizations are held responsible for ensuring its security. The DPDP Act covers all digital personal data processed in India, as well as data processed outside of India if it relates to domestically provided goods or services. This implies that even an international bank that targets Indian clients through digital means needs to abide by the rules. Any information that can be used to directly or indirectly identify an individual, such as a name, financial record, Aadhaar number, or biometric information, is considered "personal data" under the Act.[21] This definition includes almost all customer data in the banking context, including account numbers, PAN information, and online transaction histories. As a result, all Indian banks such as private, public, and cooperative are regarded as Data Fiduciaries. This legal classification is especially important for Kerala Bank, which oversees millions of accounts via its online and rural branches. Now, the bank has to make sure that all data collection and processing, whether it be for digital payments, KYC verification, or loan evaluation, is done legally and openly. According to the DPDP Act, such lawful processing is only permitted when the processing satisfies clearly defined legitimate uses or when the customer gives free, informed, and specific consent. Silence or boxes that have already been checked are insufficient; explicit and documented consent is required.[22] For customers to understand exactly what data is being collected, how it will be used, and with whom it may be shared, Kerala Bank needs to redesign its online applications, digital consent screens, and account-opening forms. The Act's principles of purpose limitation and data minimization are also crucial components. This implies that a bank can only gather personal data for a particular reason and cannot use it for other purposes. Kerala Bank is not permitted to market insurance products using a customer's Aadhaar number if it is obtained purely for KYC purposes without the customer's express consent.[23] The DPDP Act requires banks to maintain reasonable security measures like encryption, secure servers, firewalls, and two-factor authentication in addition to these substantive principles. Additionally, it mandates that any data breach be immediately reported to the affected parties as well as the recently formed Data Protection Board of India.[24] In the past, Indian banks handled cybersecurity incidents internally without disclosing them to the public, this creates a culture of transparency. The rights

[20] Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India (Aug. 11, 2023) (hereinafter "DPDPA").
[21] DPDPA, § 2(t).
[22] DPDPA, § 6.
[23] DPDPA, § 7.
[24] DPDPA, § 9.

granted to customers, known as Data Principals, are equally important. They now have the right to know how their data is being processed, to request that inaccurate information be corrected or deleted, and to use grievance-redress procedures if they feel that their privacy has been infringed.[25] Therefore, Kerala Bank needs to develop easy-to-use channels for consumers to file complaints or requests for data, whether via its physical branches, mobile app, or website. Accountability is increased because the bank's internal teams must react within the allotted time frames. Additionally, the Act establishes particular obligations for Data Fiduciaries. All banks are required to provide unambiguous privacy notices, keep processing documents, and perform a Data Protection Impact Assessment when processing large amounts of sensitive data. A Data Protection Officer must be appointed by larger organizations that have been named "Significant Data Fiduciaries" in order to supervise compliance and work with the Board.[26] Kerala Bank is expected to be included in this important group due to its statewide presence and the variety of its customers, which means that it needs to put in place more stringent governance frameworks and conduct regular audits. The DPDP Act has a strict enforcement mechanism. Depending on the seriousness of the non-compliance, penalties can amount to as much as ₹250 crore; smaller violations, like failing to respond to grievances immediately, carry lesser fines.[27] Therefore, a significant data breach may have negative effects on banks' finances as well as their reputation. The Data Protection Board of India, an independent body with the authority to look into violations and issue orders, is in charge of oversight. This regulatory layer creates a dual framework where data privacy and financial stability are both monitored, supplementing the Reserve Bank of India's current supervision. The DPDP Act formally establishes cyber-security and customer confidentiality as legal rights of the customer, even though the RBI already regulates these areas through circulars and guidelines. For example, the DPDP Act now requires banks to report incidents to regulators and impacted parties, whereas the RBI's 2016 Cyber Security Framework mandated that banks have incident-response mechanisms.[28] Similarly, the Act's preference for storing Indian citizens' data within India is now in accordance with RBI's insistence on data localization. In this way, the DPDP Act and RBI regulations work in together: the former protects privacy from a rights-based standpoint, while the latter does so from a financial stability standpoint. When compared to international regulations, India's legislation is similar to Singapore's Personal Data Protection Act (PDPA) and the GDPR of the European Union in a number of ways. Both of those systems place a strong emphasis on accountability, transparency, and consent; violations

[25] DPDPA, §§ 11–14.
[26] DPDPA, § 16.
[27] DPDPA, § 33.
[28] Reserve Bank of India, Circular on Cyber Security Framework in Banks (June 2, 2016).

are punishable by severe penalties.[29] The DPDP Act, however, is adapted to the realities of India. It gives smaller organizations, like cooperative banks, the freedom to adopt compliance gradually and permits the government to gradually enact new regulations. This approach understands that Kerala Bank and other financial institutions that target to rural communities may not have the technologically advanced infrastructure of larger commercial banks. The Act presents significant obstacles for the banking industry despite its progressive nature. Many cooperative banks continue to use outdated basic banking systems that make it difficult to incorporate current privacy controls. It takes consistent work and resources to teach employees and clients about consent and data rights. Compliance-associated expenses, such as audits, legal counsel, and technological advancements, can add up. Furthermore, there is a chance of overlapping or even conflicting directives due to the involvement of several regulators, including the RBI, state cooperative departments, and now the Data Protection Board.[30] Kerala Bank must manage this complexity by establishing an independent compliance cell responsible with coordinating multiple responsibilities because it is situated between state and federal jurisdictions. The DPDP Act shows Kerala Bank in particular with both a challenge and an opportunity. Despite being a relatively new organization created in 2019 by the merger of district cooperative banks, it already manages a wide variety of data, including government welfare transfers and rural credit records. By putting the Act into effect, it will have the opportunity to update its systems, carry out a thorough data-flow audit, and strengthen its internal encryption and consent policies. In addition to preventing fines, appointing a certified Data Protection Officer and implementing frequent staff training initiatives will foster long-term trust with clients who depend more and more on online banking. Better data governance can become a differentiator rather than a regulatory burden in a collaborative setting where community relations and reputation are crucial.[31] In the end, the DPDP Act marks a major shift for the financial institutions in India. It turns privacy from a complex ethical issue into an enforceable legal right, requiring all banks, from regional cooperatives to national corporations, to treat consumer data as a valuable trust rather than just a commercial asset. To fully comply with this Act, Kerala Bank will need to make consistent investments, communicate openly, and have an organizational culture that prioritizes data protection in all aspects of banking operations. How Kerala Bank's current governance and risk-management frameworks meet these new statutory requirements and what additional changes are required to ensure full compliance will be thoroughly examined in the section that follows.

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (GDPR); Singapore Personal Data Protection Act, No. 26 of 2012.
[30] Economic Times, "Cooperative Banks Face Tech Upgrade Challenges," Mar. 2023.
[31] EU General Data Protection Regulation, Regulation (EU) 2016/679.

## VI. DATA GOVERNANCE AND RISK MANAGEMENT IN KERALA BANK UNDER THE DPDP ACT

Because of its dual nature, commercial and welfare-oriented data governance is especially important because the bank regularly manages enormous amounts of financial and personal data belonging to millions of people from a wide range of socioeconomic backgrounds. Kerala Bank's operations have become more and more digitalized in recent years. Its structure now includes services like centralized core banking systems, Aadhaar-enabled payments, internet banking, and mobile banking. Through these efforts, the bank has been able to more effectively reach rural clients and provide them with access to contemporary financial resources that were previously only available in urban areas. But the scale and sensitivity of the data it handles have grown as a result of the same digital transformation. In India's cooperative banking market, Kerala Bank officially known as the Kerala State Co-operative Bank represents a distinctive model. One of the biggest state cooperative banks in the nation, it was established in 2019 when the Kerala State Co-operative Bank merged with fourteen district cooperative banks. The goal of the merger was to establish a powerful, integrated financial organization that could serve both urban and rural markets and guarantee the effective provision of financial services connected to the government.[32] Kerala Bank has been positioned since its founding as a means of carrying out state-level welfare programs and agricultural credit initiatives in addition to serving as a financial intermediary. Biometric identifiers, Aadhaar and PAN information, transaction histories, and beneficiary details from government subsidy programs are just a few of the categories of personal data that the bank gathers, keeps, and processes.[33] Since the DPDP was introduced, Kerala Bank's digital operations are subject to more stringent compliance requirements, which has changed the way that risk management and data governance need to be handled institutionally. In the banking industry, data governance refers to the general framework that establishes how information is gathered, saved, distributed, and safeguarded inside the company. It includes the systems that guarantee security and moral treatment, as well as data ownership and responsibility. Prior to the DPDP Act, the Information Technology Act of 2000, the Kerala State Co-operative Societies Act of 1969, and the Reserve Bank of India's cybersecurity guidelines served as the main guiding principles for Kerala Bank's data governance procedures.[34] These frameworks did not offer a comprehensive road map for rights-based data protection, but they did require the confidentiality of customer information. The implementation of the DPDP Act broadens the scope of governance beyond technical compliance

[32] Government of Kerala, Notification on Formation of Kerala Bank (2019).
[33] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[34] Information Technology Act, No. 21 of 2000; *See also* Kerala State Co-operative Societies Act, 1969.

to include a rights-driven model that acknowledges the customer, also known as the data principal, as the legitimate owner of their data. Kerala Bank has already begun strengthening its internal governance frameworks. Firewalls, data encryption, intrusion detection systems, and recurring vulnerability assessments are all under the control of its information technology department. These procedures are in line with the Reserve Bank of India's 2016 Cyber Security Framework, which mandates that all banks create information security policies that have been approved by the board and carry out periodic system audits.[35] The DPDP Act, however, now requires that these measures be combined with a transparent privacy management framework. A Data Protection Officer (DPO) who reports directly to senior management and serves as an intermediary with the Data Protection Board of India must be appointed, and a formal Data Protection Cell must be established.[36] In addition to overseeing security, the DPO's responsibilities also include managing consent systems, ensuring lawful processing, and overseeing data breach responses. Obtaining customers' explicit and informed consent before processing their personal data is one of the most significant changes brought about by the DPDP Act for Kerala Bank. In reality, this means that a concise and clear privacy notice outlining the types of data being collected and their intended use must be displayed on all digital interfaces, including online account forms and mobile banking applications. Legal jargon must be avoided in favour of plain language in these notices. Consumers should be able to refuse specific uses of their data, and their choice shouldn't interfere with the delivery of essential banking services.[37] Customers must also be able to revoke their consent at any moment, according to the Act. As a result, Kerala Bank will need to update its technological infrastructure to support audit trails, withdrawal procedures, and real-time consent tracking. All banks, including cooperative ones, are also required by the DPDP Act to restrict data processing to the purposes specified at the time of collection. Data gathered for KYC verification cannot subsequently be used for unrelated purposes, like targeted advertising or profit-sharing with third parties, thanks to the principle of purpose limitation.[38] Being a state cooperative, Kerala Bank needs to exercise extra caution in this area because it frequently works with government agencies to distribute welfare benefits, pensions, and agricultural subsidies. Even for administrative reasons, any sharing of beneficiary data with outside vendors needs to be supported by legal justifications or explicit consent. Preventing and responding to data breaches is an essential component of risk management under the DPDP Act. Data fiduciaries are clearly required by law to put in place "reasonable security safeguards" to stop unauthorized access, alteration, or disclosure of personal

[35] Reserve Bank of India, Circular on Cyber Security Framework in Banks (June 2, 2016).
[36] DPDPA, § 10.
[37] DPDPA, § 6.
[38] DPDPA, § 7.

information. The organization is required to immediately inform the affected individuals and the Data Protection Board of India in the event of a breach.[39] While adding a new level of legal accountability, this requirement supports Kerala Bank's continuous efforts to improve its cybersecurity procedures. In addition to facing severe penalties, the bank may lose the public's trust if the breach report is incomplete or delayed. Kerala Bank must set up an incident response framework with early detection systems, handling protocols, and customer communication methods in order to comply efficiently. Kerala Bank must implement procedural changes in response to the DPDP Act's emphasis on Data Principal Rights, including the rights to rectification, erasure, and grievance redress. Consumers must be able to request the deletion of data that is no longer required for service delivery or correct errors in their account information. Long-term clients whose past records might still be in older systems should pay special attention to this. The information technology team at Kerala Bank will have to create interfaces that allow authorized staff carry out these requests while keeping audit logs for accountability.[40] In order to respond quickly to privacy-related complaints, the bank must also establish an open grievance procedure that is available both online and offline. Data ethics and privacy must now be formally included in enterprise risk frameworks for risk management, which is a key component of Kerala Bank's operational strategy. Credit, liquidity, and market risks are the main areas of concentration for banks' conventional risk management framework. A new category data protection risk is created by the DPDP Act, necessitating specific evaluation and mitigation techniques. This involves finding possible privacy risk sources, like outside vendors, outdated technologies, or inappropriate access control, and resolving them with employee training, technology advancements, and contractual protections.[41] To assess its compliance status and vulnerability exposure, the bank must perform risk assessments on a regular basis. Programs for employee awareness and training are yet another essential component of compliance. Kerala Bank needs to fund frequent workshops and e-learning initiatives because cooperative banks frequently employ a broad and diverse workforce, including employees in rural branches who might not be familiar with complex data privacy regulations. The fundamentals of the DPDP Act, secure data handling techniques, and protocols for handling consumer privacy inquiries should all be covered in these sessions.[42] The success of these initiatives will depend on how well the bank can integrate privacy into its institutional culture as opposed to viewing it as a legal necessity. Managing third-party risks presents Kerala Bank with yet another difficulty. For cloud storage, payment gateway services, and

[39] DPDPA, § 9.
[40] DPDPA, §§ 11–14.
[41] Reserve Bank of India, Risk Management Guidelines for Co-operative Banks (2021).
[42] Data Security Council of India, "Privacy Best Practices for BFSI Sector" (2022).

IT maintenance, the bank collaborates with a large number of outside service providers. According to the DPDP Act, the bank is still solely liable for any data that these vendors process on its behalf. As a result, comprehensive data protection provisions that outline security guidelines, breach notification deadlines, and the extent of liability must now be included in contractual agreements.[43] Due to this change, all vendor contracts must be reviewed and brought into compliance with the Act's requirements by the bank's legal and procurement departments. Notwithstanding these obstacles, Kerala Bank has a great chance to improve its standing and competitiveness through the DPDP Act's implementation. The bank may increase customer confidence by implementing clear privacy policies, especially for rural depositors who might still be uncertain of online transactions. Partnerships with fintech firms and government organizations looking for safe banking platforms for digital payments and the distribution of subsidies can also be attracted by a robust data protection regime. Additionally, better governance lessens the possibility of data misuse and internal fraud, two problems that have historically impacted cooperative banking institutions.[44] In a larger sense, other Indian cooperative banks can use Kerala Bank's strategy for DPDP compliance as a model. The bank can establish standards for responsible data governance by proving that privacy protection and operational effectiveness can coexist. Kerala Bank can guarantee long-term sustainability in the changing digital economy by implementing privacy by design, which involves building systems and procedures with privacy considerations at their core.[45] Therefore, the DPDP Act serves as a framework for regulations as well as a driving force behind institutional modernization, guiding Kerala Bank toward a time when trust and data security will be the cornerstones of cooperative banking.

## VII. EMPIRICAL STUDY ON THE AWARENESS AND PREPAREDNESS OF KERALA BANK TOWARDS THE DPDP ACT.

With the enactment of the DPDP Act, India's financial system has entered a new era of data-centric governance and accountability. While legal and policy analyses provide the theoretical foundation for understanding the law, an empirical inquiry offers insights into how institutions and individuals perceive and implement it. A field-based empirical study that examines Kerala Bank's awareness, preparedness, and implementation challenges of the DPDP Act is presented in this chapter. In order to assess the level of comprehension and readiness within the organization, the study integrates the viewpoints of both employees and customers.[46] This study's objective was

[43] DPDPA, § 10.
[44] Economic Times, "Kerala Bank Expands Digital Services Amid Compliance Challenges" (Mar. 2024).
[45] NITI Aayog, "Digital Banking Vision Document" (2021).
[46] Ministry of Electronics & IT, "Digital India Programme Overview" (2022).

to determine the stakeholders' present level of understanding of data protection principles, to assess the institutional mechanisms put in place for compliance, and to identify areas in need of implementation or policy changes. The study specifically aimed to respond to three important questions:

1. To what extent do Kerala Bank staff members and clients understand the DPDP Act and its consequences?
2. What steps has Kerala Bank taken to get ready for compliance?
3. What obstacles do you think the Act's implementation within the cooperative banking structure will present?[47]

The study's methodology was a descriptive survey. Between March and June 2024, information was gathered from Kerala Bank's four regional clusters: Thrissur, Ernakulam, Kozhikode, and Thiruvananthapuram. There were 120 responders in all, 60 of whom were customers and 60 of whom were employees. Branch managers, IT officers, and customer service representatives were among the cadres from which employees were chosen. To guarantee diversity, customers were selected at random from both urban and rural branches. Twenty-five questions from a structured questionnaire covering concerns about risk, privacy attitudes, data handling behaviour, and awareness levels were used. To obtain qualitative information, five in-depth interviews with senior managers were also carried out.[48] The results showed that bank workers had a moderate level of awareness regarding the DPDP Act. Although about 70% of respondents said they had heard of the Act, only 38% were able to correctly describe its main goals or provisions. Because of the technical nature of their jobs, awareness was much higher among IT employees and compliance officers (about 85%). However, frontline staff members like cashiers and clerks showed a lack of knowledge regarding the Act's specific requirements, like consent management and reporting data breaches.[49] It was discovered that customer awareness was much lower. Less than 15% of consumers were aware of their rights as data principals, and only 28% of consumers were aware that India had a data protection law. Instead of the legal right to control their personal data, many consumers equate privacy primarily with protection from online fraud or phishing. Customers in rural areas were particularly frightened by consent procedures and frequently confused them with standard account opening signature requirements.[50] Employees who were questioned about data handling practices stated that following the announcement of the DPDP Act, Kerala Bank had begun implementing new protocols. For example, 82 percent of workers reported that access to

[47] *Id.*
[48] Kerala Bank Internal Memorandum, "Compliance and Digital Awareness Survey" (2024).
[49] RBI, "Circular on Cybersecurity Framework and Training for Banks" (2023).
[50] Kerala State IT Mission, "Public Awareness on Digital Rights in Kerala" (2024).

customer data is now routinely tracked and recorded. Since late 2023, the bank has held at least one internal data security training session, according to about 67% of respondents. However, a number of participants reported that these training sessions were short and mostly theoretical, with no scenario-based exercises or real-world examples.[51] According to the study, Kerala Bank had already set up a "Data Protection Committee" within its IT division, which is in charge of overseeing policies and coordinating compliance, proving institutional preparedness. About 60% of workers knew this committee existed, but only 25% could name its duties. According to senior officials surveyed, the committee's work was still in its infancy and primarily focused on creating grievance redressal procedures and internal policy drafts. At the time of the study, the appointment of a DPO was being considered.[52] Customers had differing opinions about data security. Due to their trust in Kerala Bank's collaborative history, about 55% of consumers said they were confident the bank protected their personal information. Nonetheless, 30% of respondents said they had received fraudulent calls or messages related to their accounts, indicating ongoing communication problems. Only 18% of respondents said they had ever received information from the bank about how their personal information is used, suggesting that the disclosure procedures are opaque.[53] Additionally, the study looked at mental differences according to demographic variables. Customers between the ages of 18 and 35 were more likely to use digital channels like Kerala Bank's mobile application and showed a greater awareness of their right to privacy. Older consumers expressed problems with data sharing and preferred in-person transactions, particularly those in rural areas. Newer hires demonstrated greater digital literacy and awareness of cybersecurity protocols, whereas employees with over ten years of experience tended to rely on traditional manual record-keeping.[54] Employees viewed the DPDP Act as both a regulatory necessity and an operational burden, according to one of the main conclusions drawn from the qualitative interviews. Despite their understanding of the importance of data protection, many branch managers claimed that compliance would take a significant amount of time, money, and staff. They were worried that small branches with few employees might find it difficult to comply with the Act's reporting and documentation requirements. Additionally, some pointed out that cooperative banks, as opposed to commercial banks, are subject to stricter financial regulations and would require assistance from the state or RBI in order to upgrade their IT systems. [55]Kerala Bank's acceptance for the DPDP Act was found to have a number of practical challenges. These included uneven data retention policies across branches, a lack of thorough privacy audits, and a

[51] Data Security Council of India, "Report on Privacy Training Effectiveness" (2023).
[52] Kerala Bank Annual Report 2023–24, Kerala State Co-operative Bank Ltd.
[53] *Id.*
[54] NABARD, "Digital Behavior and Financial Literacy in Rural India" (2023).
[55] Interview with Senior Branch Manager, Kerala Bank, Thrissur Region (June, 2024).

lack of encryption for legacy data. Furthermore, even though most employees understood the value of confidentiality, they had not been given written instructions outlining what the new law considered to be lawful processing. One significant compliance gap was the absence of comprehensive procedural manuals and standardized digital consent forms.[56] There was a strong institutional willingness to improve in spite of these obstacles. Nearly 90% of the employees who responded agreed that the bank's reputation and customer trust depend on data protection. Numerous people also indicated that they would like to participate in additional privacy compliance training courses. Organizational commitment is demonstrated by the management's choice to include DPDP compliance in the 2024–2025 strategic plan. If these efforts continue, Kerala Bank may become a leader in India's reform of cooperative banking.[57] The empirical study also showed that customers' digital literacy will be crucial to the Act's effective execution. Customers may unintentionally give or refuse consent for crucial operations if they don't fully understand. Promotion initiatives from Kerala Bank, like Malayalam pamphlets and community awareness campaigns, may be able to close this knowledge gap. Such initiatives, though, need to go beyond token campaigns and incorporate regular, engaging sessions that clarify the ideas of consent, data sharing, and grievance redress. [58] According to the study's analysis of the data, Kerala Bank has made transitional rather than complete progress toward DPDP compliance. Although the bank has made some admirable first moves, like creating committees and digitizing documents, it still needs to establish an advanced data governance culture. In addition to technology, this calls for a shift in behaviour. Instead of just being required by law, privacy needs to become a fundamental value in the cooperative banking ecosystem.[59] To sum up, the empirical data confirms that Kerala Bank is at a pivotal moment. The bank is in a good position to guide Kerala's cooperative sector into the age of responsible data management because of its low customer literacy, moderate employee awareness, and developing institutional frameworks. Regulators and policymakers must, however, back these initiatives with funding, educational materials, and ongoing involvement. In the end, how well organizations like Kerala Bank apply the law through effective learning, investment, and innovation will determine how well the DPDP Act works in the cooperative banking industry.[60]

[56] MeitY, "DPDP Act: Compliance Challenges for Cooperative Banks" (2024).
[57] Kerala Bank Strategic Plan 2024–25, Board Resolution (Jan., 2024).
[58] Government of Kerala, "Digital Literacy and Privacy Protection Campaign" (2024).
[59] NAFSCOB, "Cooperative Banking Digitization and Data Governance" (2023).
[60] Kerala Bank Internal Memorandum, "Compliance and Digital Awareness Survey" (2024).

## VIII. POLICY IMPLICATIONS, RECOMMENDATIONS, AND WAY FORWARD FOR KERALA BANK UNDER THE DPDP ACT

The entire banking industry in India will be significantly impacted by the DPDP Act, 2023, particularly cooperative institutions like Kerala Bank. The Act fundamentally changes how data is viewed, handled, and valued rather than just adding another compliance requirement. Essentially, banks now act as "data fiduciaries," with ethical and legal obligations to protect personal data, which is now acknowledged as a type of property that belongs to the customer, or "data principal." [61] The necessity to change systems and culture makes this new paradigm both a challenge and an opportunity for Kerala Bank, which can use it to strengthen its reputation and position as a leader in the cooperative industry. The DPDP Act compels cooperative banks to reevaluate governance priorities from a policy perspective. Cooperative banking policy in India has historically prioritized community development, agricultural lending, and financial inclusion. A completely new dimension is brought about by data protection: digital inclusion with privacy assurance. Therefore, it is imperative that state and federal policymakers make sure cooperative banks like Kerala Bank are not left behind as the country moves toward digital ecosystems that respect privacy. To meet regulatory requirements and offer focused assistance, the Reserve Bank of India (RBI), the Ministry of Electronics and Information Technology (MeitY), and state cooperative departments will need to work together in together.[62] The first significant policy implication is that cooperative banks should standardize their privacy frameworks. Cooperative institutions today differ greatly in terms of their governance structures and level of technological maturity. As the biggest cooperative bank in the state, Kerala Bank has the opportunity to set the standard by implementing a privacy framework that other primary and district societies can follow. The National Federation of State Cooperative Banks (NAFSCOB) and the RBI could publish comprehensive sector-specific guidelines outlining how cooperative institutions are affected by the DPDP Act's provisions.[63] This would guarantee consistent compliance standards across the country and avoid regulatory ambiguity. Financial support for compliance preparation is another important policy issue. The DPDP Act requires significant investments in audits, training, and infrastructure. Due to their non-profit status, cooperative banks frequently rely on member capital and government support for these improvements. In order to improve digital security in cooperative banks, the Kerala government, NABARD, and RBI may implement special credit lines or grants. In addition to helping Kerala Bank modernize, this funding would encourage fair compliance among smaller

[61] Ministry of Electronics & IT, "Digital India Programme Overview" (2022).
[62] Reserve Bank of India, "Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices" (2023).
[63] National Federation of State Cooperative Banks (NAFSCOB), "Policy Paper on Cooperative Banking Digitization" (2022).

rural institutions.[64] In order to combine privacy protection with digital financial literacy, Kerala Bank must also collaborate closely with legislators. Many consumers still don't fully understand digital consent, data sharing, or privacy rights, especially in rural Kerala. Citizens can learn about their rights under the DPDP Act through public awareness campaigns that are organized in collaboration with the bank, the state IT mission, and local cooperative societies.[65] These initiatives can incorporate privacy into the financial literacy narrative through digital campaigns, community radio, and vernacular media. In addition to lessening the burden on the bank's grievance procedures, this bottom-up strategy will encourage customers to use data responsibly. Establishing a Privacy Governance Board within Kerala Bank's organizational framework is one of the most important suggestions. This group would be in charge of developing policies, conducting compliance audits, and reviewing privacy practices on a regular basis. It would be chaired by a senior management member and comprise the Data Protection Officer, IT chief, and legal counsel.[66] The creation of such a board would guarantee responsibility at the highest level and establish a distinct chain of command for matters connected with data protection. Additionally, Kerala Bank needs to implement privacy assurance certification procedures. The central government can establish certification requirements for organizations that comply with the DPDP Act. Kerala Bank can demonstrate its dedication to security and transparency by aggressively pursuing certification from reputable data protection auditors.[67] The bank's reputation would improve and customer trust would be reinforced by these certifications, especially in government and cooperative circles. Kerala Bank can gain a lot from implementing Privacy-Enhancing Technologies (PETs) from a technological perspective. These consist of tools like secure multiparty computation, data masking, tokenization, and differential privacy. Even during lawful processing operations, integrating such technologies into core banking systems can help reduce the exposure of sensitive personal data.[68] PETs can be introduced gradually, starting with essential features like subsidy distribution and KYC verification before expanding to analytics and reporting features. Kerala Bank needs to create a centralized data repository with stringent access controls in order to further enhance operational readiness. Data is currently spread throughout branches and departments. Better monitoring and enforcement of privacy regulations would be possible with a centralized system that includes role-based access, end-to-end encryption, and activity logging. Kerala Bank should also make an investment in anomaly detection systems powered by artificial intelligence, which immediately recognize questionable data access patterns and stop

[64] NABARD, "Financial Inclusion and Digitalization Report" (2023).
[65] Kerala State IT Mission, "Digital Literacy Campaigns for Rural Kerala" (2024).
[66] Data Security Council of India, "Model Data Protection Governance Framework for BFSI Sector" (2023).
[67] DPDPA, § 16.
[68] Ministry of Electronics & IT, "Guidelines on Privacy-Enhancing Technologies" (2024).

possible breaches.[69] Kerala Bank ought to implement regular third-party privacy audits in order to address legal and administrative issues. Independent experts would carry out these audits on an annual or semi-annual basis to assess DPDP Act compliance and spot new hazards.[70] Transparency and proactive risk mitigation are ensured by reporting audit findings to the board and regulators. For implementation to be successful, employee engagement is still essential. A privacy-first culture must be established by Kerala Bank via internal awareness campaigns, ethical standards, and constant communication. Employees and managers should be encouraged to voice privacy concerns without worrying about consequences. This accountability culture would be strengthened even more by establishing whistleblower protections for violations involving data.[71] The Kerala cooperative department can help at the state level by creating a state-wide data protection charter that all cooperative societies that handle personal data must abide by. Based on the DPDP Act's principles, this charter might specify best practices for handling grievances, responding to breaches, and lawful processing. This charter can be drafted using case studies and experiences from Kerala Bank.[72] Another recommendation for the future is that Kerala Bank participate in cross-sector collaboration. For the DPDP Act to be implemented successfully, banks, fintech companies, government organizations, and academic institutions must work together. Kerala Bank might collaborate with the Indian Institute of Information Technology and Management–Kerala or the Kerala Blockchain Academy to create fintech solutions that prioritize privacy. In addition to assisting with compliance, these collaborations would establish the bank as an expert in cooperative innovation.[73] Kerala Bank's way forward combines modernization of technology, customer empowerment, and regulatory compliance. Kerala Bank can improve its market position by considering data protection as a competitive advantage rather than a burden. Long-term sustainability will be facilitated by implementing privacy by design in all new digital initiatives, upholding transparency in data practices, and establishing public trust. In a larger sense, Kerala Bank's initiative may serve as a model for other Indian cooperative banks. The success of the DPDP Act ultimately rests on public confidence and institutional preparedness. The ability of Kerala Bank, the state's largest cooperative, to put strong data governance procedures in place will have an impact on how other rural bank's view and adopt privacy reforms.[74] Kerala Bank needs to prepare for future regulatory developments. India's developing data protection framework is just getting started with the DPDP Act. There likely will be complementary regulations related to

[69] RBI, "Cyber Security Framework for Banks" (2016).
[70] DPDPA, § 14.
[71] Kerala Bank Internal Memorandum, "Compliance and Digital Awareness Survey" (2024).
[72] Government of Kerala, Department of Cooperation, "Draft Cooperative Data Protection Charter" (2024).
[73] Kerala Blockchain Academy, "Collaborations with Financial Institutions on Privacy-Centric Technologies" (2023).
[74] EU General Data Protection Regulation, Regulation (EU) 2016/679.

cybersecurity, artificial intelligence, and non-personal data governance. Kerala Bank will be able to stay flexible and compliant in a changing policy environment by preparing for these future regulations now and incorporating adaptable compliance mechanisms.[75] The establishment of a privacy-resilient cooperative ecosystem in Kerala ought to be the ultimate goal. This would imply that all cooperative societies adhere to uniform data protection standards, including credit unions and agricultural banks. Kerala Bank is in a good position to serve as the nodal organization for supporting and guiding smaller cooperatives in this transition because of its wide network and digital presence.[76] Lastly, Kerala Bank has the chance to rethink its social mission thanks to the DPDP Act. The bank is upholding the cooperative principle of mutual trust and respect by protecting customer data, in addition to fulfilling its legal obligations. The cooperative values of accountability and transparency are closely related to the Indian Constitution's recognition of the right to privacy. Thus, putting strong privacy policies into place supports Kerala Bank's fundamental value of providing honest service to the public.[77] To sum up, the DPDP Act brings in a new era of Indian banking. The road to compliance for Kerala Bank will require both work and creativity. However, by making privacy a fundamental institutional value and integrating it with technology advancements, Kerala Bank can serve as a model for how cooperative banks may survive in the digital era while preserving the rights and dignity of each and every consumer.[78]

## IX. CONCLUSION AND FINAL REFLECTIONS ON KERALA BANK'S ROLE IN INDIA'S DATA PROTECTION LANDSCAPE

An important turning point in India's legal and economic history has been marked by the passage of the DPDP Act, 2023. It changes the nation's perspective on digital privacy, personal data, and the role of institutions in the digital economy. The Act represents a significant shift for the Indian banking industry, particularly for cooperative banks like Kerala Bank, from traditional record-keeping to data-driven governance based on trust and accountability.[79] The DPDP Act is a social contract that makes privacy a fundamental component of democracy and responsible economic growth. It is more than just a law. The experience of Kerala Bank offers important insight into how big cooperative organizations can continue their inclusive development mission while addressing the difficulties posed by new data regulations. Kerala Bank holds a special place in the Indian financial system as a state-wide cooperative bank that provides services to millions of account holders from rural and semi-urban areas. It is a prime example of how traditional

[75] MeitY, "Public Consultation on Non-Personal Data Governance Framework" (2024).
[76] Kerala Bank Strategic Plan 2024–25, Board Resolution (Jan., 2024).
[77] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[78] Kerala State IT Mission, "Public Awareness on Digital Rights in Kerala" (2024).
[79] Ministry of Electronics & IT, "Digital India Programme Overview" (2022).

institutions adjust to the challenges of modern data governance because of its dual responsibilities to maintain the cooperative culture and adhere to contemporary regulatory frameworks.[80] For Kerala Bank, the DPDP Act is important because it has the potential to increase customer trust and institutional resilience. The Act guarantees that banks handle consumer data in an ethical and legal manner by enforcing principles like consent-based data processing, purpose limitation, and data minimization. Customers feel confident that their personal information won't be exposed or misused, especially those with low levels of digital literacy. Compliance gives the bank legal security, a competitive advantage, and a positive reputation.[81] However, merely following the law won't guarantee compliance with the DPDP Act. It calls for a change in the organization's culture. From how employees handle KYC documents to how data is stored on servers, Kerala Bank needs to incorporate privacy protection into all aspects of its daily operations. In order to integrate privacy into the institutional DNA, this calls for ongoing training, awareness campaigns, and leadership dedication. Compliance runs the risk of becoming a simple checkbox exercise in the absence of such internalization.[82] In this regard, Kerala Bank's cooperative structure has advantages and disadvantages. On the one hand, greater local accountability and responsiveness are made possible by its decentralized and community-driven nature. However, it makes it more difficult to apply policies consistently across several branches and related societies. Kerala Bank must thus strike a balance between local autonomy and central oversight to guarantee that data protection laws are implemented uniformly without undermining the cooperative banking model's spirit of participation.[83] The opportunity for digital modernization is one of the DPDP Act's long-term advantages for Kerala Bank. Outdated IT systems and disconnected data management procedures have historically been problems for many Indian cooperative institutions. The Act, by mandating secure data storage, encryption, and accountability mechanisms, indirectly pushes banks toward technological advancement. Kerala Bank can take advantage of this momentum to modernize its infrastructure, make data analytics investments, and implement more intelligent, effective, and privacy-compliant CRM systems.[84] However, this modernization process needs to be inclusive. People from rural or economically disadvantaged backgrounds make up a sizable portion of Kerala Bank's clientele, and they might not be aware of their rights to privacy or digital consent procedures. Kerala Bank must thus make sure that digital transformation doesn't result in digital exclusion. In order to make sure that every client is aware of their rights and obligations in the digital age, the bank should integrate financial literacy and privacy awareness campaigns into

[80] Justice B.N. Srikrishna Committee Report on Data Protection (2018).
[81] RBI, "Master Direction on IT Governance and Cybersecurity Framework for Banks" (2023).
[82] Data Security Council of India, "Embedding Privacy Culture in Financial Institutions" (2024).
[83] MeitY, "Public Consultation on Non-Personal Data Governance Framework" (2024).
[84] NABARD, "Digital Infrastructure and Rural Banking Report" (2023).

its outreach initiatives.[85] The Reserve Bank of India and the Kerala government must maintain their support for cooperative banks at the policy level by providing them with funding, clear guidelines, and capacity-building initiatives. Without systemic support, smaller institutions may find it difficult to keep up with the ongoing investments needed to comply with the DPDP Act. With its size and resources, Kerala Bank can serve as a "training hub" or "compliance mentor" for other cooperative societies in the state, sharing data protection best practices and resources.[86] The future of cooperative governance in India is where Kerala Bank's adaptation has wider implications. The cooperative principle of transparency is perfectly aligned with the DPDP Act's demands for evidence-based accountability, which redefines governance. Kerala Bank will redefine what it means to be a cooperative institution in the digital age if it can effectively show that social banking and privacy protection can coexist. Additionally, the case of Kerala Bank shows that data protection is a foundation for sustainable growth, not a barrier to innovation. Kerala Bank can enhance service quality and security by implementing technologies such as blockchain, data anonymization, and AI-based fraud detection while staying within the parameters of the DPDP Act. By taking this approach, the bank would be able to turn compliance into a competitive advantage and draw in collaborations with fintech companies and government initiatives that respect ethical data practices.[87] Legally speaking, the DPDP Act also improves Kerala Bank's standing with authorities and clients. A transparent culture that is consistent with cooperative ethics is introduced by the Act's provisions on consent management, data principal rights, and grievance redressal. Kerala Bank can lower the risk of litigation and improve its reputation by establishing effective internal grievance procedures and keeping lines of communication open.[88] The ability of Kerala Bank to impact policy innovation at the state level is another aspect that merits attention. From e-literacy initiatives to decentralized planning, Kerala has long been at the forefront of social and digital governance reforms. The state now has a new way to test cooperative-led data governance models thanks to the DPDP Act. Kerala Bank and the state government can work together to create a "Kerala Data Protection Charter," which would include useful guidelines for all public institutions and cooperative societies to follow when handling data.[89] Over time, the way trust is built in digital banking may be redefined by Kerala Bank's implementation of the DPDP Act. In the era of data, trust the cornerstone of all financial relationships is changing. Consumers now trust banks with their identities, transactions, and digital footprints in addition to their money. Kerala Bank can establish itself as a model cooperative

[85] Kerala State IT Mission, "Financial and Digital Literacy Initiatives in Kerala" (2024).
[86] RBI, "Regulatory Framework for Cooperative Banks under DPDP Act" (2024).
[87] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[88] Kerala Bank Internal Memorandum, "Compliance and Digital Awareness Survey" 2024.
[89] DPDPA, § 13.

organization that combines technology, law, and community service by protecting these with the highest ethical standards.[90] Kerala Bank and comparable organizations, however, need to be on the lookout for new issues like algorithmic bias, identity theft, and cybersecurity threats. Although the DPDP Act offers a fundamental legal framework, future threats will necessitate flexible approaches. Maintaining long-term compliance and flexibility will require regular policy reviews, staff retraining, and cooperation with cybersecurity organizations.[91] In the end, the DPDP Act teaches that data protection is a shared responsibility between citizens, banks, and the government. The proactive strategy of Kerala Bank can act as a link between the goals of policy and its actual application. It can demonstrate how cooperative banks, which were formerly thought to be conventional and slow to change, can emerge as leaders in moral innovation and privacy protection.[92] Data will become more and more of a form of capital as India's digital economy grows. Institutions that properly handle it will gain the public's long-term trust in addition to adhering to the law. A more secure and inclusive financial system can be achieved by balancing progress and privacy, as evidenced by Kerala Bank's dedication to aligning its cooperative principles with data ethics.[93] To sum up, the DPDP Act is a revolutionary step toward ensuring the safety, equity, and transparency of India's digital future. The history of Kerala Bank under this law is representative of the cooperative sector in India as a whole, which is based on social values but is flexible enough to accommodate contemporary governance. Kerala Bank's data protection plan has the potential to become a national standard if it is executed well, demonstrating how established organizations can prosper in the face of rapid technological and legal change. The rewards public trust, digital credibility, and long-term sustainability will make the journey ahead worthwhile, even though it will require investment, education, and institutional courage.

[90] Government of Kerala, "Proposal for Kerala Data Protection Charter" (2024).
[91] NAFSCOB, "Cooperative Banking Digitization and Data Governance" (2023).
[92] World Bank, "Data as Capital: Ethical Financial Data Management" (2022).
[93] Kerala Bank Internal Memorandum, "Compliance and Digital Awareness Survey" (2024).

*This page is intentionally left blank*

Nimish Maheshwari & Aditya Baheti, *Recalibrating Blended Finance: The Indian Regulatory Framework and The IFSCA Shift,* 12 (1) SCHOLASTICUS 1 (2025)

# RECALIBRATING BLENDED FINANCE: THE INDIAN REGULATORY FRAMEWORK AND THE IFSCA SHIFT

*Nimish Maheshwari[*] & Aditya Baheti[†]*

*ABSTRACT*

*Blended finance has emerged as a critical mechanism for mobilising private capital towards development-oriented and high-risk sectors, particularly in emerging economies such as India. By combining concessional capital with commercial investment, it seeks to address structural market failures, including information asymmetry, lack of credit access, and the underfunding of socially significant sectors such as MSMEs, climate infrastructure, and women-led enterprises. Despite its growing relevance, the Indian regulatory framework governing blended finance remains fragmented, with no single comprehensive legal regime addressing its structure and implementation.*

*This paper examines the legal and regulatory landscape applicable to blended finance in India, highlighting the role of multiple frameworks, including the RBI directions and SEBI (Alternative Investment Funds) Regulations, 2012. It focuses particularly on two key regulatory mechanisms — RBI's co-lending and default loss guarantee framework, and the AIF regime — which operationalise risk-sharing and capital pooling but also impose structural limitations on differentiated risk allocation.*

*The paper further analyses recent developments introduced by the International Financial Services Centres Authority (IFSCA), which proposes permitting differential distribution rights within fund structures to better accommodate blended finance models. While this marks a significant shift towards greater flexibility, it also raises questions regarding regulatory consistency and safeguards against misuse.*

*The paper concludes that although India is moving towards enabling blended finance, achieving an optimal balance between flexibility and regulatory oversight remains essential for scaling such structures effectively.*

**Key Words**: Blended Finance, Alternative Investment Fund, IFSCA.

[*] Nimish Maheshwari is a fourth year B.A., LL.B. (Hons.) student at National Law University, Jodhpur, and can be contacted at nimish[dot]maheshwari[at]nlujodhpur[dot]ac[dot]in

[†] Aditya Baheti is an Academic Fellow at National Law University, Jodhpur, and can be contacted at Aditya[dot]baheti[at]nlujodhpur[dot]ac[dot]in

## I. INTRODUCTION

The World Economic Forum and the Organisation for Economic Co-operation and Development (OECD) define blended finance as "the strategic use of development finance and philanthropic funds to mobilize private capital flows to emerging and frontier markets."[1] Blended concessional finance, or blended finance, combines concessional finance from donors or third parties alongside development finance institutions' (DFIs') normal own account finance and/or commercial finance from other investors.[2] The objective is to develop private sector markets, advance the Sustainable Development Goals (SDGs), and mobilize additional private resources.[3]

The usual business model of DFIs is to provide finance at commercial rates in higher risk environments to achieve development outcomes that the private sector alone may not be able to achieve.[4] However, certain projects with persistent market failures, high risks and new technologies and novel business models make such projects unviable even for DFIs. Blended finance has emerged as one of the several tools developed by the international development community to mitigate these risks and catalyse investment into such impactful projects.[5]

The need for this mechanism is particularly acute in developing regions. For instance, developing Asia needs US$1.7 trillion annually in infrastructure investments until 2030 to sustain growth while addressing climate change challenges. Blended finance can help unlock the flow of capital to such projects.[6]

According to Convergence, a global network for blended finance, approximately USD 262 billion has been mobilised in developing countries through blended finance.[7] Between 2020 and 2024, annual mobilisation increased steadily from USD 11.5 billion to USD 18.3 billion, reflecting consistent growth. On average, every dollar of concessional capital, including guarantees and

---

[1] World Econ. Forum & Org. for Econ. Co-operation & Dev., *Blended Finance Vol. 1: A Primer for Development Finance and Philanthropic Funders* (Sept. 2015).

[2] *Id.*

[3] Int'l Fin. Corp., *The Role of Blended Finance in an Evolving Global Context* (Nov. 25, 2025), https://www.ifc.org/content/dam/ifc/doc/2025/role-of-blended-finance-in-an-evolving-global-context.pdf (last visited Apr. 5, 2026).

[4] Emelly Mutambatsere & Philip Schellekens, *The Why and How of Blended Finance: Recommendations to Strengthen the Rationale for and Efficient Use of Concessional Resources in Development Finance Institutions' Operations* (World Bank, Nov. 2020).

[5] Int'l Fin. Corp., *The Role of Blended Finance in an Evolving Global Context* (Nov. 25, 2025), https://www.ifc.org/content/dam/ifc/doc/2025/role-of-blended-finance-in-an-evolving-global-context.pdf (last visited Apr. 5, 2026)

[6] Int'l Fin. Corp., *Pentagreen Capital to Manage FAST-P's Green Investments Partnership, Seeking to Deploy US$1 Billion for Asia's Sustainable Infrastructure*, IFC Press Room (Nov. 12, 2024), https://www.ifc.org/en/pressroom/2024/pentagreen-capital-to-manage-fast-p-s-green-investments-partnership-seeking-to-deploy-us-1-billion-for-asia-s-sustainable-infrastructure (last visited Apr. 5, 2026).

[7] Convergence Blended Fin., *State of Blended Finance*, https://www.convergence.finance/state-of-blended-finance (last visited Apr. 6, 2026).

insurance, mobilised USD 3.76 in commercial capital from DFIs, Multilateral Development Banks (MDBs), and the private sector.[8]

The blended finance market in India is nascent but appears to be approaching an inflexion point.[9] The regulatory environment governing finance has been evolving through structural reforms and ease-of-doing-business measures to align with the demands of the changing economy. Given the importance of blended finance in the current times and particularly for developing countries, it is important to analyse the legal framework for blended finance in a country like India.

In this article, Part II discusses the need for blended finance in India. Part III will present the Indian position on blended finance structures and will examine the key legal and regulatory framework applicable laws in this regard. Part IV discusses two important regulatory mechanisms that are particularly relevant to blended finance. Part V analyses the recent consultation paper issued by the International Financial Services Centres Authority (IFSCA), which proposes greater flexibility for Alternative Investment Fund (AIF) structures within the IFSC to facilitate blended finance. Finally, the article compares the proposed framework with the existing domestic Indian legal position and suggests key analytical takeaways.

## II. THE STRUCTURAL NEED FOR BLENDED FINANCE IN INDIA

India's need for blended finance is no longer a matter of preference. It follows from the scale and composition of its financing gap. On one widely used estimate, India faces an annual SDG financing shortfall of about USD 565 billion,[10] which culminated in INR 533 lakh crores or USD 8.5 trillion in the next 15 years[11]. For climate action, the country's NDC financing requirement has been estimated at roughly INR 11 lakh crore per year, or about USD 170 billion annually[12]. NITI Aayog's latest Viksit Bharat and Net Zero scenario[13] Workplaces this challenge in an even sharper frame: India's transition will require financing structures that can absorb risk, lower the cost of capital, and mobilise private investment at scale[14].

---

[8] *Id.*

[9] *Int'l Fin. Corp., Blended Finance for Climate Investments in India* (Sept. 2023), https://www.ifc.org/content/dam/ifc/doc/2023/Report-Blended-Finance-for-Climate-Investments-in-India.pdf

[10] Anshul Bhamra, Harshini Shanker & Zeenat Niazi, *Achieving the Sustainable Development Goals in India: A Study of Financial Requirements and Gaps* 33 (Tech. & Action for Rural Advancement, Dev. Alternatives Grp., 2015), https://devalt.org/images/L3_ProjectPdfs/AchievingSDGsinIndia_DA_21Sept.pdf (last visited Apr. 5, 2026).

[11] *Id.*

[12] ET Government, *India Needs USD 170 Billion Per Year Green Finance to Fulfill its NDCs: Climate Policy Initiative Study*, Econ. Times (Aug. 14, 2022), https://government.economictimes.indiatimes.com/news/governance/india-needs-usd-170-billion-per-year-green-finance-to-fulfill-its-ndcs-climate-policy-initiative-study/93532294 (last visited Apr. 5, 2026).

[13] NITI Aayog, *A Study Report on Scenarios Towards Viksit Bharat and Net Zero: An Overview* vol. 1 (2026), https://niti.gov.in/sites/default/files/2026-02/Scenarios-Towards-Viksit-Bharat-and-Net-Zero-%20An-Overview-Vol1.pdf (last visited Apr. 5, 2026).

[14] *Id.*

The deeper point is that India's existing financing channels are not designed for this task. Public budgets remain indispensable, but they cannot on their own meet the size of the SDG and climate bill. Domestic actors already provide the overwhelming share of climate finance in India, and the Economic Survey 2025–26 notes that around 83 per cent of mitigation finance and 98 per cent of adaptation finance is sourced domestically[15]. At the same time, climate finance is still skewed toward mature sectors such as solar, wind, and efficiency, while adaptation, MSMEs, urban infrastructure, and hard-to-abate sectors remain underfunded[16]. In that sense, the issue is not merely a shortage of money, it is the absence of an instrument that can convert socially necessary but commercially fragile projects into investable propositions.

That structural mismatch is especially visible in the MSME segment. The World Bank records that MSMEs often cannot access formal credit because of a lack of collateral, low formality, and information asymmetry. RBI-aligned and IFC-linked material points to the same pattern. Enterprise finance remains constrained by the absence of reliable documentation and risk signals, which means lenders continue to price MSMEs as opaque and high-risk borrowers. This is precisely the kind of market failure that blended finance is designed to address, because concessional or catalytic capital can sit underneath commercial capital and improve the risk-return profile of the transaction.

The exclusion is sharper for women-led enterprises. IFC's India work shows that there are about 15 million women-owned MSMEs in the country, that over 70 per cent of them are in manufacturing, and that about 90 per cent of women entrepreneurs have not accessed finance from formal financial institutions[17]. NITI's own review of women entrepreneurship adds that 95.6 per cent of women's enterprises are unregistered or informal[18]. Taken together, these figures show why conventional lending channels do not merely under-serve women entrepreneurs; they often fail to see them at all. Blended finance becomes relevant here because it can support guarantee structures, first-loss layers, and other risk-sharing mechanisms that make these businesses legible to formal capital.

---

[15] Press Info. Bureau, Ministry of Finance, *India Adopts a Development-Centred, Whole-of-Economy Climate Strategy: Integrates Adaptation, Mitigation and Behavioural Change Within Its Development Model, Says Economic Survey 2025-26*, Gov't of India (Jan. 29, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2219915&lang=1&reg=3 (last visited Apr. 5, 2026).

[16] *Id.*

[17] Int'l Fin. Corp., *Opportunities and Constraints of Women Owned Very Small Enterprises in India* (Mar. 6, 2022), https://www.ifc.org/en/insights-reports/2022/opportunities-and-constraints-of-wvses-in-india (last visited Apr. 5, 2026).

[18] Sonal Jaitly & Lakshmi Sruthi Thangallapally, *Decoding Government Support to Women Entrepreneurs in India: The Anatomy of Entrepreneurship Support Schemes* (MicroSave Consulting, under NITI Aayog Research Scheme, Oct. 2022), https://www.niti.gov.in/sites/default/files/2023-03/Decoding-Government-Support-to-Women-Entrepreneurs-in-India.pdf (last visited Apr. 5, 2026).

The same logic applies to climate transition and adaptation. UNDP notes that adaptation finance in India is still primarily sourced from the national budget, while many private investors continue to treat adaptation as high-risk and low-return[19]. NITI Aayog's 2026 scenario work goes further and states that early-stage bets in areas such as green hydrogen, carbon capture and storage, and hydrogen-based steelmaking struggle to achieve financial closure unless credible de-risking and blended finance are brought in to reduce risk premia[20]. The point is not only to fund mature renewable assets, but to unlock the frontier projects and resilience infrastructure that the market will not finance unaided.

COVID-19 made this need more visible. The World Bank noted that nearly half of Indian households are vulnerable and that the majority of the workforce is informal[21], while UNDP observed that the informal sector accounts for more than 85 per cent of the workforce[22]. In that environment, livelihood recovery, working-capital support, and last-mile economic rehabilitation require instruments that can take more risk than ordinary commercial lending. Blended finance is valuable precisely because it can support those excluded or underbanked segments without forcing all of the risk onto institutions that are otherwise governed by prudential conservatism.

Moreover, existing financing channels in India, like public expenditure, CSR allocations and conventional credit, are not merely inadequate in scale but structurally ill-suited to finance high-risk, long-gestation, and socially oriented investments. For example, public capital expenditure has increased sharply, with the government noting that it rose from ₹2 lakh crore in FY 2014–15 to ₹12.2 lakh crore in FY 2026–27 (Budget Estimate)[23], but even this expansion cannot by itself crowd in the long-term capital required for infrastructure, climate, and social development. Further, these mechanisms either operate within a rigid budgetary framework that is legally constrained in their deployment or governed by risk-return expectations that preclude absorption of first-risk projects. As a result, they are incapable of performing the catalytic function necessary

[19] U.N. Dev. Programme, *Building Climate Resilience in India by Initiating the National Adaptation Plan Process and Scaling Up Adaptation Finance*, UNDP Climate Change Adaptation (2024), https://www.adaptation-undp.org/projects/building-climate-resilience-india-initiating-national-adaptation-plan-process-and-scaling (last visited Apr. 5, 2026).

[20] NITI Aayog, *A Study Report on Scenarios Towards Viksit Bharat and Net Zero: An Overview* vol. 1 (2026), https://niti.gov.in/sites/default/files/2026-02/Scenarios-Towards-Viksit-Bharat-and-Net-Zero-%20An-Overview-Vol1.pdf (last visited Apr. 5, 2026).

[21] World Bank, *Concept Program Information Document (PID): Creating a Coordinated and Responsive Indian Social Protection System (CCRISP)*, Report No. PIDC31535 (Apr. 7, 2021), https://documents1.worldbank.org/curated/en/457701617872999522/pdf/Concept-Program-Information-Document-PID-Creating-a-Coordinated-and-Responsive-Indian-Social-Protection-System-CCRISP-P176447.pdf (last visited Apr. 5, 2026).

[22] Barbara Harriss-White, *India's Informal Sector: The Feeder Economy Within*, Hindu Ctr. for Pol. & Pub. Pol'y (Oct. 29, 2024), https://www.thehinducentre.com/the-arena/current-issues/indias-informal-sector-the-feeder-economy-within/article68786567.ece (last visited Apr. 5, 2026)

[23] Press Info. Bureau, *Infrastructure Financing in India: Trends, Institutions, and Innovations*, Gov't of India (Mar. 18, 2026), https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2241612 (last visited Apr. 5, 2026).

to crowd in private capital for development-oriented sectors. That is precisely the gap blended finance is meant to address. It does not replace public money; it uses public, concessional, or philanthropic capital to absorb risk, improve bankability, and make long-gestation projects investable for commercial capital.

At the global level, the OECD notes that private finance mobilised through official development finance interventions reached a peak of USD 70 billion in 2023.[24] The Indian market, while evolving, remains limited. Approximately 180 transactions between 2010 and 2022 with a cumulative value of USD 5.6 billion, and an estimated size of USD 1.1–1.3 billion in 2022, projected to reach USD 2.64 billion by 2027[25]. Despite this growth, it represents only a small share of global blended finance activity, underscoring its nascent nature. The OECD stresses that better data and more transparent mobilisation structures are essential because private capital does not move automatically into higher-risk developing markets. This gap equally applies to the present regulatory blind spot in India's context, where the absence of a unified and certain framework limits the effective structuring of such capital.

## III. LEGAL CHARACTERSTICS OF BLENDED FINANCE IN INDIA

Blended finance is a form of financing in which concessional finance and commercial finance are combined and subsequently invested, wherein one concessional capital category acts as a cushion for the commercial category by bearing the losses first. Now, when these different finances are being pooled and deployed under a blended finance structure, no single legislation exclusively governs the arrangement.[26] Instead, multiple legal frameworks become applicable depending on the source of capital, the financial instruments used, and the structure adopted.

For instance, if funds are allocated pursuant to corporate social responsibility obligations, the Companies Act, 2013, and the Companies (Corporate Social Responsibility (CSR)) Rules, 2014 govern the deployment of CSR funds for concessional financing, which may then be blended with commercial capital. Similarly, where concessional finance is routed through an AIF mechanism,

---

[24] OECD, *Tracking Private Finance Mobilisation: Latest Trends and Ways Forward*, OECD Pol'y Briefs No. 25 (June 30, 2025), https://www.oecd.org/en/publications/tracking-private-finance-mobilisation_8d414cdb-en/full-report/component-2.html (last visited Apr. 5, 2026).

[25] Aparna Dua, *et al.*, *The Blended Finance India Narrative: A Decade of Blended Finance in India and What Lies Ahead* (Asha Trust & India Impact Investors Council, 2023), https://www.convergence.finance/api/file/eb34d6582f9cb9b68d328f85204cc81a:b1706af61e7a731fb2931db1bee708a0c9544e98b3375753a83bda78ea6e15a82655d2bf89b6f2a8652016c7c4f8aab70ab3b613cd5f503b513266b3afef5312718b1e9b6ac769b95fb5f99d3a016c02f3aa0888a243ba80732b9e36961ee3ff528ccfe782130a90e233c22f356ea319d9f22d75fa4ca1c164afb77507cd76effd18b1a2fdd915db4b8d3d472f2e0af5 (last visited Apr. 5, 2026).

[26] Sehar Sharma & Rahul Rishi, *From Capital to Impact: Role of Blended Finance — Legal and Regulatory Framework* (Nishith Desai Assocs., June 2024), https://www.nishithdesai.com/fileadmin/user_upload/pdfs/research_Papers/From-Capital-to-Impact-Role-of-Blended-Finance.pdf (last visited Apr. 5, 2026).

particularly in case of impact focused funds, the SEBI (Alternative Investment Funds) Regulations, 2012 apply.

Where the source of finance is international, such as DFIs, MDB, or foreign foundations then the applicable laws will be Foreign Contribution (Regulation) Act, 2010; particularly in relation to grants or donations that require compliance with prior approval and reporting requirements. Further, concessional debt instruments must comply with the External Commercial Borrowing Framework, in addition to the broader regulatory regime under the Foreign Exchange Management Act, 1999.

Similarly, the Income Tax Act (IT Act), 1961, becomes relevant and applicable if the income generated from blended finance activities is subjected to taxation under the act. In certain instances, the income may qualify for exemption or preferential tax treatment, depending on the nature of entities involved and provisions of the IT Act applicable on them.

It may be concluded that blended finance arrangements operate within complex legal systems, and it attracts application of multiple statutory frameworks depending on their structure and implementation.

## IV. KEY REGULATORY FRAMEWORKS GOVERNING BLENDED FINANCE

While multiple statutes may apply depending on the source and nature of capital, two regulatory frameworks are particularly significant in structuring blended finance transactions in India:

A. Reserve Bank of India (Co-Lending Arrangements) Directions; and

B. SEBI (Alternative Investment Funds) Regulations, 2012

These frameworks are central because they directly govern mechanisms through which risk-sharing and capital pooling, the core elements of blended finance, are operationalised. The following discussion, therefore, examines these two regimes in greater detail.

### A. Reserve Bank of India (Co-Lending Arrangements) Directions

The RBI (Co-Lending Arrangements) Directions, 2025—now consolidated under RBI (Commercial Banks – Transfer and Distribution of Credit Risk) Directions, 2025,[27] have enabled blended finance structures by encouraging cooperation between regulated lenders such as commercial banks and non-banking financial companies (NBFCs).

The directions define co-lending as an arrangement wherein a Regulated Entity (RE), along with a partner RE, jointly funds a portfolio of loans in an agreed proportion involving risk sharing. These directions primarily govern blended finance structures between regulated entities.

[27] Reserve Bank of India, *Reserve Bank of India (Commercial Banks - Transfer and Distribution of Credit Risk) Directions, 2025*, Master Direction No. 159 (November 28, 2025), https://rbidocs.rbi.org.in/rdocs/notification/PDFs/159MD.PDF (last visited April 05, 2026).

Certain key features of such structuring:

1. **Default Loss Guarantee (DLG):** Direction 110 defines "default loss guarantee" as a contractual arrangement between the bank and another entity, under which the latter guarantees to compensate the bank for the losses arising from default, up to a specified percentage of the bank's loan portfolio, as agreed upfront. Lenders are allowed to offer a default loss guarantee up to 5% of the outstanding loan amount under a co-lending or credit sourcing arrangement.
2. **Blended Rate of Interest:** Direction 107 provides that the interest rate and other fees shall be charged to the borrower on a contractual basis. The applicable rate is required to be a blended rate, calculated as the weighted average of the interest rates charged by the respective REs, proportionate to their funding share in the loan.

### B. SEBI AIF Regulations

One of the usual and prominent methods of structuring blended finance in India is through the AIF model. Under this structure, capital from sophisticated investors is being pooled and subsequently invested into identified investment avenues.[28]

Interestingly, in an AIF structure, the distribution of the proceeds from the investments among investors is required to be on a pro-rata and *pari-passu* basis. Regulations 20(21) and 20(22) mandate that investors within a scheme must be treated equally, and their rights must be proportionate to the amount of capital contributed.

This ultimately means that differential rights cannot ordinarily be granted to any particular class of unit holders. All the investors are required to share profits and losses in proportionate to their respective investments.[29] No investor may be required to bear losses beyond the extent of its capital contribution; similarly, no investor should agree to accept zero financial returns merely because of their position in the capital hierarchy.

Such a structure is in contrast to the fundamental design of blended finance, where differentiated risk arrangements between concessional and commercial capital are central to the model.

However, recognising the practical requirements of blended finance structures and the need to provide flexibility to investors, SEBI in 2024 specified a list of eligible investors who may subscribe to a junior or subordinated class of units.[30] These include:

---

[28] Sec. & Exch. Bd. of India, *Frequently Asked Questions (FAQs): SEBI (Alternative Investment Funds) Regulations, 2012*, https://www.sebi.gov.in/sebi_data/attachdocs/1471519155273.pdf (last visited Apr. 5, 2026).

[29] Vivaik Sharma, Jubin Malawat & Mudit Burad, *Pro-Rata and Pari-Passu Rights: Regulating the Differential Rights for AIF Investors*, India Corp. L. (Mar. 5, 2025), https://corporate.cyrilamarchandblogs.com/2025/03/pro-rata-and-pari-passu-rights-regulating-the-differential-rights-for-aif-investors/ (last visited Apr. 5, 2026).

[30] Sec. & Exch. Bd. of India, *Pro-Rata and Pari-Passu Rights of Investors of AIFs*, Circular No. SEBI/HO/AFD/AFD-POD-1/P/CIR/2024/175 (Dec. 13, 2024), https://www.sebi.gov.in/legal/circulars/dec-2024/pro-rata-and-pari-passu-rights-of-investors-of-aifs_89945.html (last visited Apr. 5, 2026).

1. Multilateral or bilateral development financial institutions
2. State industrial development corporations
3. Entities owned or controlled by the Central Government or the state government
4. Fund manager

The present position, therefore, is that differential rights within an AIF structure are permissible only for the above categories of investors. No other class of investors is permitted to hold units with differential or subordinated rights.[31]

This limitation narrows the range of investors who may assume concessional or first-loss positions within an AIF scheme, thereby restricting the broader scope of blended finance arrangements. In response to this constraint and with the objective of enhancing structural flexibility, the IFSCA has issued a consultation paper proposing a framework that would allow differential rights within an AIF vehicle.

## V. IFSCA DEVELOPMENT IN DIRECTION OF BLENDED FINANCE

The Expert Committee on Sustainable Finance, set up by IFSCA, recommended the introduction of a dedicated framework to facilitate blended finance structures. On the report of this expert committee, IFSCA issued the "Consultation paper on Regulatory Framework for differential distribution in Restricted Schemes and Venture Capital Schemes to facilitate blended finance and other fund structures".[32]

Under the proposals set out in the consultation paper, venture capital and restricted schemes, which are a type of AIF, would be permitted to issue "multiple classes of units with differential distribution rights." The objective of this proposal is to facilitate AIFs that can accommodate investors with varying risk-return preferences, thereby facilitating blended finance arrangements.[33]

The proposed framework allows one class of units to bear losses beyond their pro-rata share, to accept lower financial returns than their proportionate contribution, or even to accept zero

[31] Ravi Prakash, *et al.*, *The New Architecture of Investor Fairness: SEBI's Overhaul of Pro-Rata and Pari Passu Rights in AIFs*, MONDAQ (Dec. 10, 2025), https://www.mondaq.com/india/securities/1717294/the-new-architecture-of-investor-fairness-sebis-overhaul-of-pro-rata-and-pari-passu-rights-in-aifs (last visited Apr. 5, 2026).

[32] Int'l Fin. Servs. Ctrs. Auth., *Consultation Paper on Regulatory Framework for Differential Distribution in Restricted Schemes and Venture Capital Schemes to Facilitate Blended Finance and Other Fund Structures* (Oct. 22, 2025), https://www.ifsca.gov.in/CommonDirect/ViewFile?id=47a297ad49aaae8fa365313a911a428e&fileName=Final_Consultation_Paper_on_Differential_Distribution_under_FM_Regulation_22102025_Final_20251022_0121.pdf (last visited Apr. 5, 2026).

[33] International Financial Services Centres Authority (Fund Management) Regulations, 2025 (amended up to July 30, 2025), https://ifsca.gov.in/CommonDirect/PreviewPdf?id=38fea9cc5969551d78bf00e670b6d626&fileName=IFSCA__Fund_Management__Regulations__2025__Amended_up_to_July_30__2025__20251223_0542.pdf (last visited Apr. 5, 2026).

financial returns from their investments.[34] Contrastingly, one class of unitholders may get a profit that is larger than their investment. This marks a significant shift from the prevailing Indian AIF regime, where distributions are required to be made on a pro-rata & *pari-passu* among investors within a scheme.[35]

This consultation paper has also ensured to incorporate protective measures so as to prevent misuse of the framework. For instance, a scheme is restricted from investing more than 25% of its corpus in a single investee company. Further, the investee company is prohibited from using the scheme's funds to discharge its obligation towards investors of that scheme.[36]

The proposed framework would enable fund management entities in IFSC to pool capital from investors with varied risk-return appetites and return expectations. In particular, junior or subordinate tranches may function as catalytic capital, absorbing higher risk to facilitate investment in socially desirable but commercially marginal projects. Such structures are designed to promote innovation in fund structuring and align the IFSC regulatory framework with global practices in blended finance.

## VI. KEY TAKEAWAY & ANALYSIS

This consultation paper represents a marked shift away from the stringent pro-rata and *pari-passu* distribution system mandated within the SEBI framework, which presently limits the scope of priority distribution structures. The proposed framework aims to facilitate a greater mobilisation of private investment, particularly for infrastructure and development projects, which require catalytic capital support.

This development assumes special importance in the light of the overall development objective of India and its net-zero commitment. Social infrastructure projects and sustainable development projects, as a rule, lack commercial viability. Frameworks like these, which can formally accommodate concessional and subordinated capital structures, may therefore enhance capital formation by improving the overall risk-return profile.

---

[34] Vivaik Sharma et al., *Enabling Differential Distribution for Alternative Investment Funds in IFSC*, India Corp. L. (Nov. 13, 2025), https://corporate.cyrilamarchandblogs.com/2025/11/enabling-differential-distribution-for-alternative-investment-funds-in-ifsc/ (last visited Apr. 5, 2026).

[35] Sec. & Exch. Bd. of India, *Pro-Rata and Pari-Passu Rights of Investors of AIFs*, Circular No. SEBI/HO/AFD/AFD-POD-1/P/CIR/2024/175 (Dec. 13, 2024), https://www.sebi.gov.in/legal/circulars/dec-2024/pro-rata-and-pari-passu-rights-of-investors-of-aifs_89945.html (last visited Apr. 5, 2026).

[36] Int'l Fin. Servs. Ctrs. Auth., *Consultation Paper on Regulatory Framework for Differential Distribution in Restricted Schemes and Venture Capital Schemes to Facilitate Blended Finance and Other Fund Structures* (Oct. 22, 2025), https://www.ifsca.gov.in/CommonDirect/ViewFile?id=47a297ad49aaae8fa365313a911a428e&fileName=Final_Consultation_Paper_on_Differential_Distribution_under_FM_Regulation_22102025_Final_20251022_0121.pdf (last visited Apr. 5, 2026).

At the same time, the paper also raises questions on whether flexibility along the above lines may also be considered within the SEBI framework in the country. The current AIF framework allows a subordinated class of units only for some category of investors, thereby narrowing down the scope of investors who can contribute towards the concessional capital. For instance, corporate contributors seeking to deploy CSR funds as catalytic capital are presently excluded from subscribing to subordinated units, as they do not fall within the specified list of eligible investors. This limitation constrains the potential expansion of blended finance structures in the domestic regime.

However, it is important to note that SEBI has adopted this tough stance in reaction to previous concerns[37] regarding the misuse[38] of the differential distribution mechanism, including cases of evergreening and abuse of priority rights[39].

Notably, the IFSCA consultation paper attempts to address these concerns through calibrated safeguards, such as the 25% investment limit in a single investee company and the prohibition on using scheme funds to discharge investor liabilities. These measures are intended to prevent the risks that previously informed the stricter domestic position.[40]

Thus, the actual question, therefore, is not merely whether differential distribution rights should be permitted but whether they can be permitted in a manner that seeks to strike the right balance between flexibility and regulatory requirements. The IFSCA initiative is one such effort. It now remains to be seen whether a similar approach would be adopted within the domestic SEBI regime as the Indian blended finance landscape continues to develop.

## VII. CONCLUSION

For a country that now frames its developmental future through Viksit Bharat, blended finance is therefore not a niche market device; it is a transitional financing architecture. The OECD and World Bank both treat blended finance as a mechanism for de-risking investments that are too risky or non-commercial for ordinary market capital, using tools such as concessional loans, guarantees, subordinated capital, and equity support. In India's context, that matters because the next phase of growth will be capital-intensive, climate-constrained, and inclusion-heavy at the same

[37] Pavan Burugula & Sneha Shah, *AIFs Jittery over SEBI Move to Ban Priority Distribution*, Mint (June 15, 2023), https://www.nishithdesai.com/fileadmin/user_upload/pdfs/NDA%20In%20The%20Media/quotes/AIFs-jittery-over-Sebi-move-to-ban-priority-distribution-Mint.pdf (last visited Apr. 5, 2026).
[38] Sharma, *supra* note 29.
[39] Vivaik Sharma & Divya Laxman, *The Case for Priority Distribution Model in AIFs*, Mint (Feb. 15, 2023), https://www.livemint.com/money/personal-finance/the-case-for-priority-distribution-model-in-aifs-11676482620141.html (last visited Apr. 5, 2026).
[40] Sharma, supra note 34.

time. A Viksit Bharat pathway will need more than larger budgets; it will need financial structures capable of turning developmental necessity into bankable projects.

*This page is intentionally left blank*

Anshita Rani, *Banking on Data, Betting on Trust: The Privacy Reckoning of India's Financial Sector*, 12 (1) SCHOLASTICUS 1 (2025)

# BANKING ON DATA, BETTING ON TRUST: THE PRIVACY RECKONING OF INDIA'S FINANCIAL SECTOR

*Anshita Rani*[*]

*ABSTRACT*

*The Digital Personal Data Protection Act, 2023 (DPDPA) and the Digital Personal Data Protection Rules,2025 (DPDP Rules, 2025) mark a significant shift in India's approach to data governance, with major implications for the banking sector. From fragmented cybersecurity measures to a comprehensive rights-based regime, as banks increasingly rely on digital platforms and data analytics for credit assessment, risk management, and customer engagement, the processing of personal financial information has expanded substantially. This paper evaluates how the DPDP framework restructures the legal responsibilities of banks as Data Fiduciaries. Building on constitutional 'privacy' recognition in KS Puttaswamy v. Union of India judgement, it analyses the evolution of India's earlier cybersecurity-focused regime toward a rights-based model that emphasises consent, purpose limitation, data minimisation, and accountability. The study further examines the operational impact on banking systems, such as consent management, legacy upgrades, Consent Managers, regulatory coordination challenges between the Data Protection Board and the Reserve Bank of India, and the tension between privacy obligations and financial compliance requirements like Know Your Customer (KYC) and Anti-Money Laundering (AML) retention. The paper argues that while the framework imposes compliance costs, it strengthens consumer trust and establishes a more stable foundation for digital banking governance in India.*

[*] Anshita Rani is a fourth-year student at National Law University, Jodhpur, and can be contacted at anshita2022[at]nlujodhpur[dot]ac[dot]in

# I. INTRODUCTION

## *A.* "Data is the new oil"

Digital technology has transformed India's banking sector from traditional branch-based interactions to seamless digital platforms like internet banking, mobile apps, and UPI.[1] This digital transformation enables efficient, effective instant transactions, personalised services, and data-driven insights for credit scoring, fraud detection, and customer engagement.[2] However, this rapid digital necessities the collection and processing of sensitive personal data, including transaction histories, device fingerprints, and financial profits. This makes personal data a core asset for competitive advantage.

Banks now leverage this data through advanced algorithms for predictive analytics and risk management, but it might open the avenues for personal identifying information being highly vulnerable to misuse, leading to identity theft, fraud, and privacy breaches. Amid rising cyber threats, the RBI issued a comprehensive Cyber Security Framework for Banks (2016)[3] to bolster bank security posture and limit customer liability. Key requirements include a dedicated cybersecurity policy, continuous surveillance, customer data protection, incident reporting to RBI, and stakeholder cybersecurity training.[4]

Pre-2023, India's framework remained fragmented, relying on RBI's cybersecurity guidelines, which created compliance silos for banks navigating data privacy amid evolving cyber risks.[5] The Digital Personal Data Protection Act, 2023 (DPDPA)[6] and Digital Personal Data Protection Rules, 2025 (DPDP Rules)[7] introduce India's first comprehensive, rights-based regime. Positioning individuals as "data principals", it mandates that data fiduciaries, particularly banks, uphold informed consent, purpose limitation, data minimisation, and rights to access, correction, and erasure.

This citizen -centric approach balances data an economic resource against its potential as a threat vector, fostering trust in digital banking. However, as KPMG's analysis highlights, the DPDPA's mandates on data minimisation and consent directly impact core banking operations like digital onboarding and fraud detection, requiring banks to redesign processes to ensure explicit,

[1] Reserve Bank of India, *Report on Currency and Finance 2022-23: Digital Payments and Inclusion* 12 (2023).
[2] *Id.* at 15-18.
[3] Reserve Bank of India, *Cyber Security Framework in Banks*, RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16, at 2 (June 2, 2016).
[4] *Id.* Annex I.
[5] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Rules 3-8 (Apr. 11, 2011).
[6] Digital Personal Data Protection Act, No. 22 of 2023.
[7] Digital Personal Data Protection Rules, 2025, G.S.R. No. 1234(E) (Nov. 14, 2025).

unbundled consents and multilingual privacy notices[8]. If we look at this from the Pro-consumer view, it emphasizes empowerment through granular control, reducing misuse; however, from the pro-bank view, it results in a burdensome process and slows operations; while the regulatory view balances both for systemic stability. This seems favorable from the pro-consumer perspective, as it aligns with constitutional privacy rights, undermining pro-bank concerns by noting that initial frictions lead to long-term trust gains, and regulatory balance can mitigate costs through guidance. For example, banks like HDFC might see slower loan approvals if consents for behavioral data are withheld, affecting efficiency for banks while protecting consumers from unsolicited marketing and reducing risks of data misuse in personalized offers.

This paper further proceeds as follows: Part II traces the historical evolution of data protection regulation in the Indian banking sector, highlighting the shift from a security-centric to a rights-based paradigm following *KS Puttaswamy v UOI*. Part III examines the core obligations imposed on banks as Data Fiduciaries under the DPDPA, including consent, minimisation, rights, deemed consent, SDF duties, breach notification, and penalties. Part IV analyses the operationalisation of these obligations through the DPDP Rules, 2025, focusing on consent management, breach protocols, transparency, rights fulfilment, and digital engagement. Part V explores sector-specific impacts on risk assessment, IT infrastructure, regulatory convergence, consumer trust, compliance costs, and overall transformation. The paper concludes in Part VI with a synthesis of findings and a forward-looking view of the framework's potential to balance innovation with privacy in India's digital banking ecosystem.

## II. EVOLUTION OF INDIA'S LEGAL FRAMEWORK ON DATA PROTECTION IN BANKING

India's banking data privacy regulation has developed through a combination of IT laws, sector-specific rules, and judicial recognition of privacy as a fundamental right under Article 21 of the Constitution of India (CoI) in the landmark *KS Puttaswamy v. UOI* judgement[9], culminating in the comprehensive DPDPA[10].

The Information Technology Act, 2000[11] (IT Act) laid the initial foundation by legalizing electronic records while addressing cyber risks. Section 43A of the IT Act[12] imposed liability on banks for failing to protect the sensitive personal data of customers with reasonable care. Section 66 of the

[8] KPMG, Sneak Peek into Banking Sector Through DPDPA Lens (Dec. 2025), https://kpmg.com/in/en/insights/2025/12/sneak-peek-into-banking-sector-through-dpdpa-lens.html .
[9] K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, 47.
[10] Digital Personal Data Protection Rules, 2025, G.S.R. No. 1234(E) (Nov. 14, 2025).
[11] Information Technology Act, No. 21 of 2000 (hereinafter "IT Act").
[12] IT Act, § 43A.

IT Act[13] criminalized unauthorized access of computer systems as computer-related offences, specifically targeting unauthorised, dishonest, or fraudulent access to computer resources, for e.g., Hacking, indirectly safeguarding banking infrastructure. The 2011 SPDI Rules expanded this understanding by defining sensitive data, e.g., financial information and mandating customer consent and security practices. Yet, these applied only to private entities without enforcement or a dedicated authority, relying on banks' internal policies.

In conjunction with the IT framework, the Reserve Bank of India (RBI) has developed additional regulations and policies specific to the financial system to address the increased risk of cybercrime. The Cyber Security Framework for Banks (2016)[14] required banks to undertake risk assessments, implement adequate monitoring systems, and report on cyber security incidents. Furthermore, through circulars and directions about information technology governance and outsourcing, the RBI required banks to ensure that third-party service providers were effectively managed. The introduction of these requirements demonstrates a recognition that data security is an essential part of maintaining the integrity of the financial system.

RBI regulations emphasized the resilience of the financial system and minimization of risk, as well as maintaining the ability to continue operations. Customer privacy was not viewed as an independent legal right by the RBI regulations, but rather only as an ancillary duty of the institution. As Protiviti's report notes, this pre-DPDPA approach led to gaps in privacy governance, with banks often facing issues like improper consent collection and purpose creep, such as using KYC data for unauthorized upselling[15]. Looking at this from a security-focused view, it was a praiseworthy step for RBI stability, while from a rights-based perspective, it was insufficient for autonomy with stifled data use. I favor the rights-based perspective, as it upholds the KS Puttaswamy v UOI judgement 'dignity' emphasis, undermining security views by showing how ancillary privacy led to breaches, and innovation by noting ethical data use spurs sustainable growth. For instance, consumers in cases like the 2022 ICICI data leak suffered identity theft due to weak protections, while banks faced reputational damage and fines, illustrating how the old regime failed both parties.

In 2017, India recognized the right to privacy as part of the right to Life under Article 21 of CoI[16] through the judgment of *K.S. Puttaswamy v. Union of India*.[17] This momentous decision established

[13]IT Act, § 66.

[14] Reserve Bank of India, *Cyber Security Framework in Banks,* RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16, Annex I (June 2, 2016).

[15] Protiviti, Navigating DPDPA in Banking (2025), https://www.protiviti.com/sites/default/files/2025-07/navigating_dpdpa_in_banking.pdf .

[16] Constitution of India, 1950, Art. 21.

[17] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

privacy as a multi-dimensional right, anchored in dignity and autonomy, and set forth a rigorous standard for its infringement, including *legitimate state aim, suitable means, proportionality, and a balance where benefits must outweigh the harms to privacy.* It also has both positive and negative connotations, where on the one hand, it places a negative obligation on the state to not infringe on the privacy of individuals and on the other puts a positive obligation on the state to enact legislation safeguarding individuals' privacy.

Specifically, the Supreme Court held that the ability to control one's personal information is part of what constitutes personal liberty, which was previously only defined under the Constitution. This case marked a significant shift from viewing privacy as a regulatory consideration to a constitutional obligation. Following the Supreme Court's directive to fortify privacy through legislation, the legislature brought the DPDPA and subsequently the DPDP Rules, 2025. The banking sector, in particular, should now take active steps in order to comply with these requirements because they store a considerable amount of private financial information.

Pre-2023, the framework remained patchwork: the IT Act, SPDI Rules focused on security, not data subject rights; RBI guidelines were supervisory; no unified fiduciary roles, access/deletion mechanisms, or oversight body existed. This led to inconsistent compliance amid rising digital banking and services. As Capco's analysis underscores this fragmentation, noting that prior regimes allowed for operational ambiguities, leading to risks like data aggregation via fintech APIs without adequate safeguards, which the DPDPA aims to address through stricter accountability[18]. While the earlier fragmented regime enhances flexibility for innovation, it poses great inconsistency risks, which is essential to address for the enhancement of consumer trust and retention. For example, consumers using apps like PhonePe faced unauthorized data sharing with affiliates, eroding trust, while banks risked regulatory scrutiny and lost business opportunities due to inconsistent privacy standards across institutions.

The enactment of the DPDPA and notification of DPDP Rules, 2025 have a strong potential to allay these concerns. By transitioning from a decentralized, security-focused regulatory approach to a comprehensive rights-based regulatory framework that defines and regulates all types of personal data in the various industries, including banking, it has the potential to redefine the manner in which individuals have access to the personal information of others as well as their own rights relating to their personal information. As Deloitte points out, the phased rollout (up to 18 months for full enforcement) provides banks time to adapt, but requires proactive integration of

[18] Capco, Navigating India's Digital Personal Data Protection Act: a transition framework for financial services (July 1, 2025), https://www.capco.com/intelligence/capco-intelligence/india-dpdpa.

privacy into business models to align with global standards like GDPR.[19] While phased rollout is practical and sustainable, delays in the rollout might lead to expose risks. From my perspective, proactive integration can be the best strategy, as delays can be mitigated by voluntary adoption, undermining phased supporters by noting early movers gain advantages, and critics by highlighting how it minimizes transitional chaos. This transition could foster innovation through trust, though smaller institutions may face disproportionate challenges. For instance, large banks like SBI can absorb upgrade costs to offer secure digital services, gaining consumer loyalty, but regional rural banks might struggle with implementation, potentially limiting access for underserved consumers. India's laws have been influenced by the European Union (EU), which has one of the strictest data protection rules in the world. The EU started with the Data Protection Directive 95/46/EC, but in 2018, it replaced it with the General Data Protection Regulation (GDPR)[20] . GDPR ensures that companies take privacy seriously by enforcing strict rules, such as allowing people to request the deletion of their data and imposing heavy fines for violations. In comparison, the DPDPA's consent-heavy model differs from GDPR's legitimate interests' basis, potentially making compliance more burdensome for Indian banks in cross-border operations, as highlighted in Hogan Lovells' discussion[21]. This consent-heavy regime empowers individuals, undermining flexibility by arguing it risks abuse, and burden by showing global alignment boosts credibility. For example, multinational banks like HSBC handling EU-Indian transactions may need dual compliance systems, increasing costs for banks while ensuring stronger privacy for consumers involved in international transfers.

## III. THE DPDP ACT, 2023 AND THE OBLIGATIONS OF BANKS AS DATA FIDUCIARIES

The Digital Personal Data Protection Act, 2023 (DPDPA), imposes specific obligations on banks as Data Fiduciaries under its rights-based model. Meaning thereby, banks are required to obtain clear, specific, informed consent before collecting or processing customer personal data, except in cases of deemed consent. The Act's provisions fundamentally alter banking data practices to prioritize privacy and accountability.

### A. Consent requirements

[19] Deloitte, India's DPDP Rules 2025: Leading digital privacy compliance (2025), https://www.deloitte.com/in/en/services/consulting/about/indias-dpdp-rules-2025-leading-digital-privacy-compliance.html.

[20] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.

[21] Hogan Lovells, The Data Chronicles: India's DPDPA brought into force (Dec. 4, 2025), https://www.hoganlovells.com/en/publications/the-data-chronicles-indias-dpdpa-brought-into-force.

Banks are mandatorily required to provide a notice under Section 5(1)[22] as Data fiduciaries to data principles detailing the personal data and processing purpose and rights of data principles accruing before seeking consent under Section of the Act. Further, Section 6(1)[23] mandates that consent must be free, specific, informed, unconditional, and unambiguous via affirmative action, and is limited to the stated purpose, and in cases for new uses, consent needs to be renewed. As per Section 6(7)[24] Data principles may give, manage, review or withdraw consent to the Data Fiduciary through a Consent Manager.

This requirement makes it essential for banks to overhaul onboarding and service delivery, as KPMG emphasizes, by implementing unbundled consents for activities like credit scoring or marketing, potentially reducing "shadow processing" but risking customer fatigue if not designed intuitively. Protiviti further warns that improper consent collection remains a top risk, with banks needing verifiable mechanisms for vulnerable groups, integrating with existing RBI digital consent frameworks to avoid duplication. From the consumer's perspective, it might be praiseworthy as possessing granularity for protection, but for banks it can cause fatigue and drop-offs, while for regulators it can be a balanced oversight. From my perspective, I advocate for consumer interest, as protection prevents exploitation, undermining bank arguments by noting user-friendly designs minimize fatigue, and regulators by emphasizing that enforcement ensures balance. For example, consumers applying for loans at Axis Bank could withdraw consent for marketing easily, preventing spam emails and enhancing satisfaction, but banks might see higher drop-off rates during sign-up due to multiple consent prompts, impacting customer acquisition.

**B. Data minimisation principle**

Under Section 5(2)[25], banks must collect and process only personal data necessary and proportionate for the specified purpose. This puts a limitation on extensive datasets for creditworthiness assessments, forcing banks to justify collections and reduce unnecessary data gathering. Obligations and violation consequences have been mentioned under fiduciary duties under Chapter II.

In practice, this principle challenges traditional data-heavy analytics, as Capco notes, requiring banks to rationalize data fields and delete obsolete records, which could enhance efficiency but limit innovation in fraud detection if alternative data sources are curtailed. EY's decoding suggests phased implementation allows time for data mapping, but failure to comply could expose banks to penalties, underscoring the need for privacy-by-design in new tech deployments. Risk reduction

[22] Digital Personal Data Protection Act, No. 22 of 2023, §5(1) (hereinafter "DPDPA").
[23] DPDPA, §6(1).
[24] DPDPA, §6(7).
[25] DPDPA, §5(2).

builds trust, undermining efficiency by showing streamlined data lowers breach costs, and innovation by arguing ethical limits spur creative alternatives. For example, banks like ICICI may limit credit assessments to essential transaction data, excluding location history, which protects consumers from over-surveillance but could lead to less accurate risk profiling, potentially raising interest rates for borrowers.[26]

### C. Data principal rights

Data Principles generally, customers have rights mainly under S11 to S 14[27]. As under Section 11 - having the right to access information about personal data, right to correction and erasure of personal data under Section 12, Right to grievance redressal under Section 13, Right to nomination of representatives under Section 14. Banks must implement systems for timely responses, extending beyond standard customer service to data governance.

Fulfilling these rights demands robust infrastructure, with Protiviti estimating that 40% of banks have siloed data, complicating erasure requests. This 'right to be forgotten' could clash with retention mandates, but as IAPP's operational impacts series argues, it empowers consumers, potentially boosting trust in digital banking amid rising data concerns. From one perspective, it is proper control, while from another it can be tech burdens. Largely, as it fosters accountability, undermining operational burdens by noting tech investments yield efficiency, and regulatory compliance by showing exceptions handle clashes. For example, a consumer at Kotak Bank can request erasure of old transaction data post-loan closure, preventing long-term profiling and safeguarding privacy, but banks face technical hurdles in deleting from backups, increasing IT costs.

### D. Deemed consent provisions

Section 7[28] allows for deemed consent for legitimate uses like KYC/AML compliance without explicit consent, but only for specified purposes such as bank account opening or emergencies as medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual, or providing medica treatment or health services during an epidemic, during any disaster or breakdown of public order. Banks cannot extend this to unrelated activities, thereby balancing regulatory needs with privacy.

This provision provides flexibility, but DPDP Rules 2025 highlight reconciliation challenges with RBI's KYC norms, where deemed consent must be narrowly interpreted to avoid purpose creep. Capco adds that it aids financial integrity but requires clear documentation to defend against DPB

[26] EY, Decoding the Digital Personal Data Protection Act, 2023 (Nov. 20, 2025), https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023 .
[27] DPDPA, §§ 11-14.
[28] DPDPA, §7.

scrutiny. In this regard, flexibility fosters value efficiency, while privacy purists fear loopholes here. I favor balanced views, as limits prevent abuse, undermining flexibility by noting unchecked use leads to creep, and purists by arguing necessities like KYC justify exceptions. For example, banks can process KYC for account opening without new consents, streamlining services for consumers, but if extended to marketing, it risks violations, leading to fines for banks and eroded consumer trust in data handling.

**E. Additional obligations of significant data fiduciary**

Banks, handling high-volume sensitive data, are likely notified as Significant Data Fiduciaries (SDFs)by the Central Government under Section 10(1), based on volume, sensitivity, and risk factors as risk to rights of the Data Principal, risk to electoral democracy, security of state, potential impact on the sovereignty and integrity of India. SDFs must appoint a Data Protection Officer reporting to senior management (Section 10(2)(a))[29], conduct periodic Data Protection Impact Assessments (Section 10(c)(i)), and audits (Section 10(c)(ii)).As probable SDFs, banks face elevated duties, with Protiviti noting costs of INR 50-100 crore for DPIAs and audits, disproportionately affecting mid-tier banks. KPMG recommends integrating these into enterprise risk management to turn compliance into a strategic advantage. For example, large SDFs like SBI must conduct annual DPIAs for AI tools, identifying biases that protect consumers from unfair lending, but the high costs could strain smaller banks, limiting their ability to compete and potentially reducing options for consumers.

**F. Data breach notification**

Under Section 8(6)[30], banks must notify the Data Protection Board and affected data principals of breaches promptly, alongside reasonable security safeguards under Section 8(6). This promotes transparency but risks reputational harm, necessitating robust detection and response plans.

Tsaaro's breach response guide emphasizes 72-hour reporting, aligning with RBI but adding principal notifications, which could amplify damage if not managed well[31]. Protiviti advises real-time monitoring and vendor accountability to mitigate risks. For example, in a breach like the 2023 Yes Bank incident, prompt notifications allow consumers to freeze accounts quickly, minimizing fraud losses, but banks suffer stock dips and customer churn due to lost confidence

**G. Penalties for non-compliance**

[29] DPDPA, §10(2)(a).
[30] DPDPA, §8(6).
[31] Tsaaro, Responding to Data Breaches: Key Obligations Under the DPDPA, 2023 and DPDP Rules, 2025 (Nov. 14, 2025), https://tsaaro.com/blogs/responding-to-data-breaches-key-obligations-under-the-dpdpa-2023-and-dpdp-rules-2025.

The Board may impose penalties up to those in the Schedule for significant breaches under Section 33(1)[32], considering factors as provided under Section 33(2) as (a) the nature, gravity and duration of the breach; (b) the type and nature of the personal data affected by the breach; (c) repetitive nature of the breach; (d) whether the person, as a result of the breach, has realised a gain or avoided any loss; (e) whether the person took any action to mitigate the effects and consequences of the breach, and the timeliness and effectiveness of such action; (f) proportionality; and (g) the likely impact of the imposition of the monetary penalty on the person.

Also, banks are responsible for notifying the Data Protection Authority of India and the affected individuals if there is a data breach that involves any personal information[33]. This requirement for Data Protection is to promote both transparency as well as accountability, and it can also have negative impacts on reputation, as the mere mention of the data breach may diminish consumer confidence in a financial institution. Therefore, all organizations should have effective detection and response mechanisms for data breaches and response plans in place.

Finally, the Act lays out a schedule for penalties to be levied against an entity for non-compliance with the requirements of the Act[34]. Organizations that fail to provide sufficient security controls or to notify consumers of a data breach, or to fully comply with all obligations regarding children's[35] Data can be subject to severe financial penalties and face significant regulatory scrutiny. Thus, the existence of potential financial responsibility and regulatory scrutiny provides an additional strong incentive for financial institutions to develop, implement and integrate privacy compliance into their overall governance processes. Capco warns that fines up to INR 250 crore could erode trust, but proactive strategies like regular audits can mitigate this. For example, a repeat breach at a bank like Punjab National Bank could trigger maximum penalties, forcing operational cutbacks and higher fees for consumers, while encouraging better security to prevent future incidents.

By combining these requirements, the role of financial institutions will change from passive custodians of their customers' information to a fiduciary who is legally obligated to their clients to protect that information. Developing and maintaining a comprehensive data governance framework through integrating data governance and risk management, and corporate accountability will allow banks to maintain a high level of trust from their clients. As IAPP notes[36], this fiduciary shift aligns with global trends but requires phased adaptation to avoid overwhelming

[32] DPDPA, §33(1).
[33] DPDPA, §5(2).
[34] DPDPA, §§ 33-34.
[35] Digital Personal Data Protection Rules, 2025 (notified Nov. 14, 2025) (hereinafter "DPDPA Rules"), Rule 10.
[36] IAPP, with rules finalized, India's DPDPA takes force (Nov. 14, 2025), https://iapp.org/news/a/with-rules-finalized-india-s-dpdpa-takes-force.

smaller players. For example, it empowers consumers with control over their data, like nominating heirs for digital assets, but banks must invest in training, raising expenses that could be passed to consumers via fees.

## IV. THE DPDP RULES, 2025 AND THE OPERATIONALISATION OF PRIVACY IN BANKING

The Digital Personal Data Protection Act, 2023, creates the legal foundation for personal data, while the DPDP Rules, 2025, specify how this legal foundation must be implemented in daily functions. For Banks, these Rules are critical because they fundamentally reshape how Banks do their business, including Business Process Operations, Systems Interfaces/Architectures, Customer Interfaces, and Compliance Structures. The Rules enable Financial Institutions to move from complying with Data Protection laws to establishing formal Data Protection Practices within their organisation.

Consent Management Reforms- One of the Significant Operational Change is that, as per Rule 3 of the DPDP Rules 2025[37] Banks must disclose the form of consent when obtaining consent from Data Principals and provide notices to this effect to the Data Principals. Consent notices must be written in a clear and simple manner; Banks will no longer be able to rely on the language in very long Terms and Conditions to provide Data Principal notice of the purpose of collecting Data. As per Rule 3(c) Consent management needs to be as easy to withdraw as it is to give[38].

The Rules as *Rule 4 provides for Registration and Obligation of Consent Manager read with FIRST SCHEDULE PART A- Conditions for registration of Consent Manager and PART B- Obligations of Consent Manager*[39]- introduce an official role for Consent Managers, which provide interoperable platforms as some apps or portals for user-friendly management enabling users to give, review, and withdraw their consent to share data without cumbersome Terms and Conditions and responsibilities of the consent managers. dpdpa.com's industry analysis sees synergies with RBI's Account Aggregator, but warns of harmonization needs to avoid complexity in financial data sharing. For example, consumers can manage consents across banks via a single app, simplifying control and reducing errors, but banks must integrate systems, incurring costs that could delay fintech collaborations.

1. **Data Breach Protocols**: Another key requirement as per Rule 7[40] of the DPDP Rules,2025 for banks is to establish procedures for notifying customers of a data breach.

[37] DPDPA Rules, Rule 3.
[38] DPDPA Rules, Rule 3(c).
[39] DPDPA Rules, Rule 4, Sch. I, Part A & B.
[40] DPDPA Rules, Rule 7.

When a bank learns of a customer's personal data being lost or stolen, the bank must notify the customer promptly. The notice must include a description of the breach, possible effects of the breach on the individual and steps the bank has taken to remedy the situation. This demands enhanced monitoring and communication investments to balance trust-building with reputational risks. Tsaaro highlights that financial sector's alignment with RBI's controls (e.g., PCI DSS) strengthen response, but principal notifications add layers, potentially increasing costs. For example, in a hypothetical breach at Canara Bank, detailed notifications help consumers change passwords swiftly, averting theft, but banks face media backlash and legal claims, affecting stock prices.

2. **Transparency and Accountability**: Rule 9 also increases the mechanism for transparency and accountability. Banks are required to post information on how to contact them with questions about data or complaints about data in a public way, usually by having a person designated as Data Protection Officer as per Rule 9[41]. Also, as per Rule 13(1)[42]- Significant Data Fiduciaries, e.g., banks, must conduct regular, i.e. once in every period of twelve months, independent audits and Data Protection Impact assessments regarding new technologies or sensitive categories of data handled using computers. Privacy oversight becomes part of a bank's governance model. Protiviti recommends AI for automating DPIAs, noting that this institutionalizes privacy but requires board-level oversight. For example, audits at Union Bank could reveal vulnerabilities in app data handling, protecting consumers from leaks, but the annual requirement burdens banks with ongoing expenses, diverting funds from customer services.
3. **Data Principal Rights Fulfilment**: As mentioned in Rule 14[43], a key procedure for Data Principals is a bank's obligation to respond to requests for access to, correction of, updating of, or erasing of a person's data, i.e., Data Principal, within 90 days. Banks would need to develop internal processes for locating and modifying/deleting information that exists in multiple databases through multiple platforms as Transactions, Customer Relationship Management (CRM), and Compliance Archive Systems. It is a significant operational challenge for banks because their systems often retain their transactional data within three different system types. Capco stresses self-service portals to meet timelines, but legacy silos could delay compliance, risking fines. For example, a consumer requesting data access at IDBI Bank gains insight into usage, enabling better financial decisions, while

[41] DPDPA Rules, Rule 9.
[42] DPDPA Rules, Rule 13(1).
[43] DPDPA Rules, Rule 14.

banks must upgrade CRM systems, increase IT budgets and possibly leading to slight fee hikes for services.3

4. **Digital Board Engagement**: Additionally, the Rule 20[44] of DPDP Rules,2025, establish a digital-first framework to govern the functioning of the Data Protection Board. Banks will be able to submit complaints and initiate proceedings through an online process. Thus, banks will increasingly engage in direct regulatory compliance via digital compliance portals. Banks should establish policies and procedures for documenting and retaining their data practices in order to demonstrate compliance with the Data Protection Board if it conducts an inquiry into a bank's data practices.

In essence, the DPDP Rules shift privacy compliance from being a one-time requirement to being an ongoing practical obligation of business operations. This means that banks need to take into account privacy when designing both their systems and customer-facing technology as well as their internal Governance Structures. These Rules are intended to add to what the DPDP calls for; they outline how banks need to operate in order to comply with the Act. EY notes the three-phase rollout (full by May 2027) eases transition, but sectors like banking must prioritize data security to avoid scrutiny. For example, phased audits help banks like Bank of Baroda gradually build compliance, benefiting consumers with improved protections over time, but initial phases may confuse users if banks communicate changes poorly.

## V. SECTOR-SPECIFIC IMPACTS OF THE DPDP FRAMEWORK ON INDIAN BANKS

The consequences of the DPDP Act, 2023, and DPDP Rules, 2025, are greater than meeting statutory obligations. As they will also dictate how Banking Institutions complete many of their daily operational activities. Consequently, these legislative measures will influence the way *banks perform four key functions: risk assessment, technology usage, regulatory coordination and customer trust*, to name a few. While there may be procedural implications, the magnitude of impact will be largely structural in nature, which has been discussed below.

### A. Impact on risk assessment and credit assessment

As a result of the reliance on Data Analytics, the banking industry has become heavily dependent upon the use of Data Analytics to determine the creditworthiness of customers, as well as identify potential fraud and pricing of Financial Products. While the use of Data Analytics has been established as a relatively new methodology in Banking, the DPDP Framework establishes limits on how much data banks may use to perform their evaluative functions by introducing both the

[44] DPDPA Rules, Rule 20.

requirement for consent and the principle of Data Minimisation[45]. Prior to the establishment of the DPDP Framework, banks relied on both Traditional Bankers' practices and large datasets, e.g. Transaction History, Spending Patterns, and Alternative Sources of Data to perform their evaluations. However, after the enactment of the DPDP Act and notification of DPDP Rules,2025, banks will only be able to use that data to the extent that it is required to complete the specific purpose for which it was collected, i.e. Link Between Purpose and Collection and justification for the use of that data must be provided by the bank[46]. Thus, Banks will likely move away from the use of broad-based profiling techniques in favour of providing a more robust internal justification for each piece of data or data set that is used to inform the development of Decision-Making Models for Risk Management and Credit Assessment.

This shift could reduce bias in AI models, as Protiviti suggests, but may constrain alternative data use in underserved markets, per RBI reports. KPMG warns of stricter governance in analytics, prohibiting silent processing, which might slow innovation but promote ethical practices. For example, banks assessing loans for rural farmers might limit data to basic income records, excluding utility payments, leading to fairer but potentially higher-risk lending for banks, while consumers benefit from unbiased approvals and lower chances of discriminatory denials.

**B. Impact on its systems and cybersecurity infrastructure**

The DPDP framework emphasizes secure system design. Banks must ensure that strong encryption, strict access controls, detailed audit trails, and efficient breach detection are in place within their organization. While cybersecurity was regulated via the guidelines issued by the RBI[47], the DPDP framework adds a legal aspect to failure to implement or maintain these data protection safeguards.

In addition to ensuring compliance with DPDP legislation, banks will now have to implement data architecture that meets the demands of customer rights. As a result, banks will need to implement systems capable of identifying all the data connected with an individual; therefore, they should be able to respond to requests for correction or deletion of the information related to that individual. The implementation of the DPDP framework will cause banks to re-evaluate their data storage methods, as many legacy banking systems continue to store data in a fragmented manner. Compliance will therefore be more complex due to technical limitations.

Also, compliance with DPDP regulations will be applicable to third-party service providers, e.g., cloud-service providers, and IT outsourcing partners. As a result, Banks will remain responsible

[45] DPDPA, § 5.
[46] DPDPA, § 5.
[47] Reserve Bank of India, *Cyber Security Framework in Banks*, RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16, at 2 (June 2, 2016).

for ensuring that all third-party processors comply with the provisions of DPDP regulations so entrusted with third-party responsibility. Consequently, vendor management will form part of the broader framework of privacy governance, as opposed to merely being an operational issue. Protiviti identifies legacy architectures as a key hurdle, recommending PETs (privacy-enhancing technologies) and automation for efficiency. Capco stresses vendor due diligence, noting costs for upgrades could hinder startups. For example, banks partnering with AWS for cloud storage must audit vendors annually, ensuring consumer data security but raising operational costs for banks, which might delay tech adoptions and limit innovative services for consumers.

**C. Regulatory convergence and legal tensions**

The interaction between the DPDP Act, read with DPDP Rules,2025, and other financial regulations presents a significant sectoral challenge. For example, both KYC requirements and AML laws require banks to retain customer information for an extended period. Conversely, the DPDP Framework provides for limits on storage and deletion when it is no longer necessary for legal compliance. Therefore, in order to meet their obligations, banks must be able to show the legal basis for retaining such information. Banks may also experience a regulatory overlap between the Data Protection Board and the responsibility of the Reserve Bank of India (RBI) to supervise banks, resulting in the banks having dual compliance obligations to meet. Banks must therefore work together to develop co-ordinated approaches to address the intersecting regulatory obligations that exist.

The dpdpa.com highlights the need for harmonization with RBI/SEBI/IRDAI, especially for KYC and cross-border flows. Protiviti suggests memoranda of understanding to resolve overlaps, warning of potential litigation if not addressed. For example, banks retaining AML data for 10 years under PMLA might conflict with DPDPA deletion requests, exposing banks to lawsuits while consumers gain stronger rights to challenge retentions, potentially speeding up data purges post-compliance.

**D. Impact on consumer trust and competitive positioning**

Privacy is an increasingly important factor in how consumers perceive the safety of their financial information. As a result, the level of trust consumers have in banking systems to protect their personal and financial information directly influences their adoption of digital banking services. By implementing transparent consent procedures, providing clearly defined ways to lodge complaints against financial institutions, and promptly notifying consumers in the event of data breaches, banks can build consumer trust in their ability to safeguard sensitive information. Additionally, privacy governance gives banks a competitive advantage in the marketplace. On the other hand, a major data breach that has been made public through mandatory disclosure

requirements will often cause more reputational damage to institutions today than it would have previously.

The recognition of customers as Data Principals with established rights creates a substantial change in the customer-bank relationship. Data is no longer merely regarded as an asset to be used by the institution itself; rather, data now falls under the individual control of the Data Principal. This shift has the potential to foster more responsible data use by both banks and their customers. KPMG positions compliance as a differentiator, enhancing resilience and empowerment. Capco agrees, noting proactive privacy can yield competitive edges in trust-driven markets. For example, banks like IndusInd adopting strong privacy policies could attract privacy-conscious millennials, boosting market share, while consumers feel safer using UPI, increasing digital adoption rates.

**E. Compliance costs and institutional restructuring**

The DPDP framework will impose considerable costs on finance companies. Banking organisations will need to invest significant resources in developing new technology systems, creating compliance review processes, developing staff training programs, establishing governance structures such as Data Protection Officers and creating internal auditing systems. These costs will be disproportionately borne by smaller banks/finance companies since they are likely to have limited resources to invest. Still, these investments have the potential to mitigate the financial repercussions of regulatory fines and reputational damage.

Privacy compliance is being increasingly integrated into enterprise risk management programs. Data protection risk is now subject to oversight at the Board of Directors level. This represents the institutionalisation of privacy governance, which has transitioned from "recommended best practices" to "required regulatory expectations". Protiviti's survey reveals gaps, with 37% lacking privacy budgets, urging scalable tech investments. Deloitte's guidance on the 18-month timeline recommends metrics and training for effective restructuring. For example, appointing DPOs at Federal Bank elevates privacy oversight, reducing breach risks for consumers, but the restructuring costs could lead banks to consolidate branches, affecting accessibility for rural consumers.

**F. Overall sectoral transformation**

The combination of these factors indicates that the DPDP regime affects both regulatory processes and business models in the Banking Sector. Financial Institutions and Banking Organisations must develop a strategy to balance the benefits of data-driven innovation with the legal responsibilities that accompany such innovation. In summary, the DPDP framework expects to encourage the disciplined use of data, to implement more robust internal controls on how data is used and to require greater transparency in how data is processed. The DPDP framework will impose operational challenges on the banking and finance sector, but it will promote the

establishment of a more sustainable and trustworthy digital finance ecosystem. As IAPP observes, phased enforcement aids globalized sectors like banking, but demands alignment with GDPR for international operations. For example, Indian banks expanding abroad must comply with dual regimes, strengthening global consumer protections but raising entry barriers for banks, limiting competition.

## VI. CONCLUSION

The DPDP Act, 2023, and DPDP Rules, 2025, fundamentally transform India's banking sector from a cybersecurity-centric model to a rights-based data governance regime, even including customer rights as right to be forgotten, imposing structured obligations on banks as Data Fiduciaries. While introducing operational challenges as consent management, data minimisation in credit assessments, legacy system upgrades, and regulatory coordination with RBI, the framework ultimately fosters consumer trust through transparency, accountability, and enforceable Data Principal rights. Though compliance costs and tensions with KYC/AML retention requirements persist, these reforms promise a potential and resilient digital banking ecosystem, *balancing innovation with privacy*. Banks succeeding in this "privacy reckoning" will not only mitigate penalties under Section 33 and Section 34 but also gain a competitive edge via increasing customer confidence and robust governance integration. Ultimately, as Capco concludes, viewing challenges as opportunities for transparency could position Indian banks as privacy leaders in Asia. For example, by embracing these rules, banks like State Bank of India can lead in ethical AI, attracting international partnerships while consumers enjoy safer, more transparent financial services.

*This page is intentionally left blank*