

ENSURING CYBER RESILIENCE AND COMPLIANCE IN INDIA'S FINTECH SECTOR: A STUDY ON RBI'S REGULATORY FRAMEWORK

-Prof. Sanjeev Kumar Chadha¹

-Amit Kumar Singh²

Abstract

The rapid evolution of India's fintech sector has created unprecedented opportunities for digital financial inclusion, but it has also introduced challenges in security, compliance, and regulation. This paper examines the Reserve Bank of India's (RBI) comprehensive regulatory framework designed to bolster cyber resilience and enforce compliance within the fintech ecosystem. RBI guidelines, including the Master Directions on Cyber Resilience and Digital Payment Security, the Aadhaar Enabled Payment System, and frameworks for Self-Regulatory Organizations (SROs) and alternative authentication mechanisms, are analyzed. This paper aims to understand how these regulatory measures protect consumers, foster a secure fintech environment, and support the sustainable growth of the sector. The findings contribute to identifying best practices and regulatory needs critical for the robust development of India's fintech landscape.

Keywords

Digital Payments, Cyber Resilience, Data Privacy, Non-Banking Financial Companies (NBFCs), Self-Regulatory Organizations (SROs), Aadhaar Enabled Payment System (AePS)

Introduction

*"The responsibility should lie on someone, as this disease is making our country hollow and the poor is getting poorer and poorer. It will not help to just say that this is a case of cyber fraud and that the Criminals do not get caught and the customers themselves should be smart. The majority of the country's population is less educated and less intelligent, whereas cyber fraudsters are educated and very clever, in whose guise, innocent educated citizens are trapped"*³

-Justice Shekhar Kumar Yadav

India's FinTech industry has experienced remarkable growth, with a market size of \$50 billion in 2021 and projections estimating it will reach approximately \$150 billion by 2025.⁴ This expansion has been fueled largely by digital payment advancements, with the Reserve Bank of India (RBI)

¹ Professor of Law Department, School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow.

² Research Scholar of Law Department, School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow.

³ Justice Shekhar Kumar Yadav (Allahabad High Court), in case of Neeraj Mandal @ Rakesh v. State of U.P (2022 LiveLaw (AB) 11)

⁴ Raghav Dhanuka, BFSI – Fintech & Financial Services, available at: <https://www.investindia.gov.in/sector/bfsi-FinTech-financial> (last visited on 7 November 2024)

reporting a 10.94% growth in digital payments over the year ending in March 2023.⁵ The RBI's Digital Payments Index (RBI-DPI) highlights this trend, reaching 418.77 in September 2023 from 377.46 in September 2022, reflecting increased adoption across India. The National Payments Corporation of India (NPCI), developed through collaboration between the RBI and the Indian Banks' Association, has been integral to establishing India's robust payment infrastructure. One key player in this space is the Unified Payments Interface (UPI), which has driven significant growth in digital transactions. UPI, managed by NPCI, achieved a milestone of 500 million daily transactions on multiple occasions in 2024, supporting the Indian government's goal of reaching 1 billion transactions per day by 2026-27.⁶

Despite this growth, regulatory and security challenges remain in the FinTech sector. Recently, the RBI imposed a fine of INR 1.67 crores (around USD 200,000) on Ola Financial Services, the FinTech arm of ride-hailing company Ola, for failing to comply with prepaid payment instrument regulations and KYC processes.⁷ Such actions highlight the importance of regulatory adherence for FinTech companies. Moreover, security incidents underline the vulnerabilities in digital finance. WazirX, a major cryptocurrency exchange in India, recently suffered a cyber attack that targeted one of its multi-signature wallets.⁸ In response, WazirX temporarily suspended both INR and cryptocurrency withdrawals to mitigate risks. Though this incident had little impact on the broader crypto market, it underscores the need for heightened security measures within the FinTech ecosystem.

The Government of India, aiming to make India a leading global financial center, has sanctioned the establishment of International Financial Services Centres (IFSCs) in Special Economic Zones (SEZs) nationwide. India's first IFSC has been launched at Gujarat International Finance Tec-City (GIFT City)⁹ in Gandhinagar, Gujarat. Designed to bolster India's strategic position on the international stage, this center will offer a wide range of financial services to attract global capital and support diverse financial transactions. The IFSC at GIFT City is integral to India's vision of developing a modernized financial regulatory framework, aligning with the country's goal of fostering sustainable economic growth and becoming a premier global financial destination.

India's FinTech industry is booming, it faces ongoing regulatory and security challenges as it continues to grow and innovate. Therefore there is need to evaluate the present situations existing in the country to check whether the growth of the finTech industry is properly regulated or not. In this paper the role of RBI to boost the growth of finTech systems in India will be discussed.

⁵ Reserve Bank of India, RBI-Digital Payments Index for September 2023, Press Release: 2023-2024/1777 on January 31, 2024.

⁶ R. Chandra, UPI Achieves Historic Milestone with Over 15 Billion Transactions in September (Date: October 3, 2024), *available at*: <https://indianstartuptimes.com> (last visited on 7 November 2024)

⁷ Rajesh Kumar, RBI Imposes Penalties on Ola Financial Services, Manappuram Finance, Visa Worldwide for KYC Norm Violations And Unauthorized Payment Methods (30 July 2024), *available at*: <https://www.livelaw.in/> (last visited on 7 November 2024)

⁸ Sahana Venugopal, What is WazirX's legal status after a \$230 million wallet hack? (Published - September 03, 2024), *available at*: <https://www.thehindu.com/>

⁹ Jayshree Navin Chandra and Nitika Bakshi, GIFT City IFSC Platform For Fintech Startups & Sandbox Initiatives & Relaxation Under Companies Act (published on 12 Feb 2024), *available at*: <https://www.livelaw.in/> (last visited on 7 November 2024)

Definition of fintech

Fintech is a term that has emerged recently to describe the integration of technological innovations in the financial sector. It encompasses a wide range of technological advancements that influence financial services, and there is ongoing effort by regulators to establish a standardized definition. According to the Financial Stability Board (FSB) of the Bank for International Settlements, “FinTech is technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services”.¹⁰ This broad definition is designed to cover the diverse innovations within financial services enabled by technology, regardless of the type, size, or regulatory status of the firms involved.

The Basel Committee of Banking Supervision has adopted the Financial Stability Board's definition of fintech, describing it as “technologically enabled financial innovation that can lead to new business models, applications, processes, or products significantly impacting financial markets, institutions, and services”.¹¹

Fintech, or financial technology, involves using technology to enhance and streamline financial services. It includes a wide range of innovations, such as mobile payment apps that allow for quick and easy money transfers, digital wallets for secure transactions, and blockchain technology that powers crypto currencies like Bitcoin. Fintech also encompasses online-only banks that offer convenient and cost-effective banking services, peer-to-peer lending platforms that connect borrowers directly with lenders that provide automated investment management. Additionally, insurtech companies use technology to improve and personalize insurance offerings, while regtech solutions help financial institutions comply with regulations efficiently. Overall, fintech aims to make financial services more accessible, efficient, and tailored to individual needs.

Evolution of fintech

The evolution of financial technology (fintech) has been marked by significant milestones that have transformed the financial services industry. Its legal and historical journey is intertwined with technological advancements and regulatory responses to economic changes.

The origins of fintech can be traced back to the mid-20th century. In the 1950s, the introduction of credit cards revolutionized consumer spending, offering a convenient alternative to cash. This was followed by the advent of Automated Teller Machines in the 1960s, which provided customers with round-the-clock access to their funds. The 1970s and 1980s saw further advancements with the development of electronic stock trading and banks implementing new data recording systems. These innovations laid the groundwork for more complex financial technologies that emerged in subsequent decades.

The 1990s marked a significant leap forward with the rise of the Internet, which facilitated e-commerce and online brokering. Internet banking began to take shape, allowing customers to manage their finances from the comfort of their homes. PayPal, launched in 1998¹², was one of

¹⁰ Report of the Working Group on FinTech and Digital Banking, Reserve Bank of India, published on November 2017.

¹¹ Implications of fintech developments for banks and bank supervisors, Bank For International Settlements, published on February 2018

¹² available at: <https://www.paypal.com/> (last visited on 7 November 2024)

the pioneering online payment platforms, setting the stage for the explosion of fintech applications that would follow.

The early 2000s saw the proliferation of smart technology, with smartphones becoming ubiquitous. These devices, essentially powerful computers in the hands of consumers, drove the development of app-based operating systems. This period was characterized by innovation, unbundling, and the sharing of financial services. In 2009, Bitcoin, the first decentralized cryptocurrency, was introduced, marking a pivotal moment in fintech history. Bitcoin and its underlying blockchain technology promised to revolutionize financial transactions by offering a decentralized and secure method of transferring value.

The current decade has been characterized by the “rise of the robots,” where big data and artificial intelligence (AI) have begun to play a significant role in financial services. AI, leveraging vast and unconventional datasets, provides accurate predictions and personalized banking experiences. This era has seen the emergence of robo-advisors, automated platforms offering financial advice and investment management with minimal human intervention.

The modern incarnation of fintech gained significant momentum after the Global Financial Crisis¹³ (GFC) of 2008. The crisis exposed significant flaws in the traditional banking system, leading to a loss of public trust. Savings were diverted to subprime borrowing without adequate consumer protection, and many finance professionals faced job losses or pay cuts. This environment spurred innovation as fintech entrepreneurs sought to create transparent, facilitative, and economical banking services. In response to the GFC, traditional banking became subject to tighter regulations, creating opportunities for fintech companies to fill the gaps left by traditional banks. These companies offered more agile and user-friendly solutions, attracting a growing customer base disillusioned with conventional banking.

The legal landscape for fintech has evolved alongside these technological advancements. Initially, regulatory frameworks were often ill-equipped to address the unique challenges posed by fintech innovations. However, as the sector grew, regulators worldwide began to recognize the need for more comprehensive and tailored regulations. The Financial Stability Board¹⁴ (FSB) defines fintech as “technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services.” This broad definition underscores the diversity of fintech innovations and their potential impact on the financial system.

The evolution of fintech has been a journey of continuous innovation, driven by technological advancements and shaped by regulatory responses to economic changes. From the introduction of credit cards in the 1950s to the rise of AI-driven financial services today, fintech has fundamentally transformed the financial services industry, offering new opportunities and challenges for regulators and market participants alike.

¹³ John Turner, Why did the global financial crisis of 2007-09 happen? Banks & financial markets (4 Sep 2023), available at: <https://www.economicsobservatory.com/> (last visited on 7 November 2024)

¹⁴ Impact of Fintech on Macroeconomic Statistics, Joint Thirty-Eighth Meeting of the IMF Committee on Balance of Payments Statistics and Eighteenth Meeting of the Advisory Expert Group on National Accounts (March 7–10, 2022), BOPCOM VM1—22/03 SNA/M1.22/03, Prepared by the Financial and Payments Systems Task Team (FITT), International Monetary Fund.

Rbi and fintech regulation

The fintech landscape in India has been vibrant and transformative, driven by rapid technological advancements and innovative financial solutions. However, this growth has not been without challenges, particularly concerning financial misbehaviors and irregularities. According to the Reserve Bank of India's (RBI) Annual Report for 2021–2022, there were 3,596 reported cases of fraud involving cards and online banking in that fiscal year, marking a 34% year-on-year increase. With an average of 83 financial fraud complaints per hour, incidents such as fraudulent UPI transactions, e-wallet thefts, KYC leaks, and lending app fraud have significantly eroded public trust in the fintech sector.

Recognizing these issues, the RBI has taken decisive steps to regulate and oversee the fintech industry. Multiple rounds of stakeholder consultations have resulted in the establishment of comprehensive regulations aimed at curbing dishonest practices. The regulatory framework for fintech in India is managed by several key bodies, including the RBI, Ministry of Finance, Insurance Regulatory and Development Authority of India (IRDAI), and Securities and Exchange Board of India (SEBI).

Recently, the RBI introduced guidelines on digital lending¹⁵ to combat the growing issue of digital loan fraud. To protect borrowers' data privacy, the regulator has enhanced information-related regulations. New card-on-file (CoF) tokenization norms were implemented to address cyber fraud involving debit and credit card data misuse. Tokenization replaces sensitive payment credentials, like card numbers and security codes, with unique tokens.

The Digital Personal Data Protection Act, 2023 (DPDP Act), added further regulatory scrutiny for fintech companies handling sensitive financial data and personal identifiable information (PII). This Act outlines several obligations to ensure user data's safety and security.

Additionally, a draft framework for a Self-Regulatory Organisation (SRO) has been proposed. This framework aims to create statutory guardrails to protect the interests of customers, the economy, and fintech players. Self-regulation will empower entities to establish industry standards and best practices proactively. The SRO will set standards, maintain oversight, enforce regulations, develop the sector, and address grievances, demonstrating trust in the sector and encouraging it to uphold high standards.

As a result, unintended delays, defaults, and lapses occur, leading to potential financial and reputational risks. Over the past few years, there have been numerous cases where continuous non-compliance has prompted the RBI to take strict actions against various banks, NBFCs, and fintech companies. For a considerable period, the RBI highlighted significant non-compliance issues with Paytm Payments Bank (PPB). In 2018, the RBI temporarily suspended new account openings for PPB due to non-compliance with KYC norms, and in 2022, it completely barred new accounts citing 'certain material supervisory concerns.' The RBI has imposed significant restrictions on Paytm Payments Bank effective March 1, 2024, barring it from engaging in any banking activities, including deposits, credit transactions, wallet top-ups, and bill payments.

As organizations expand, their compliance obligations grow rapidly. Moving to digital compliance management ensures timely, transparent, and accurate adherence to regulations. Digital compliance tools offer paperless repositories, dynamic workflows, automated alerts, timely reports, and regular statutory updates. The digitization of compliance processes now includes automation, which greatly reduces costs. Automation aids in tasks like preparing returns and

¹⁵ Guidelines on Digital Lending, Reserve Bank of India, RBI/2022-23/111 DOR.CRE.REC.66/21.07.001/2022-23 (date of issue September 02, 2022).

registers, saving both time and money. Advances in regulatory technology improve corporate compliance monitoring and automate document generation for various regulators, enhancing accuracy and reducing manual effort.

FinTechs have driven the digital economy's growth but have also raised governance concerns due to their rapid expansion. Facing evolving regulations, they are adopting technology to manage business and compliance needs. RegTech solutions improve the efficiency and effectiveness of compliance programs, eliminating manual-induced errors and giving senior management better control and accountability.

Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators

The Reserve Bank of India (RBI) recently introduced Master Directions titled “Cyber Resilience and Digital Payment Security Controls”¹⁶ for non-bank Payment System Operators (PSOs), issued under Section 10(2) read with Section 18 of the Payment and Settlement Systems Act, 2007.¹⁷ Effective from July 30, 2024, these directives apply to all authorized non-bank PSOs and aim to strengthen the safety and security of digital payments by setting a robust framework for cyber resilience and risk management. Recognizing the interconnected nature of the digital payment ecosystem, the directions emphasize PSOs’ responsibility to ensure that unregulated entities within their network, such as payment gateways, third-party service providers, and vendors, also adhere to the prescribed cybersecurity standards, formalized through mutual agreements and backed by Board-approved organizational policies.

A range of specific areas is covered under the new directions, addressing various aspects of cybersecurity and digital payment security.¹⁸ They emphasize network security to prevent unauthorized access, application security measures across all stages of software development, and regular security testing to detect and address vulnerabilities. The guidelines further require stringent vendor risk management protocols¹⁹ to mitigate third-party risks and include comprehensive data security standards to safeguard sensitive information. Provisions for managing software patches²⁰ and system changes are outlined, with a focus on minimizing any security lapses. The directions also mandate PSOs to develop incident response and business continuity plans ensuring rapid recovery in the event of cybersecurity incidents and minimizing service disruption.²¹ Additional requirements include secure management of Application Programming Interfaces (APIs), regular employee training on cyber threats, and cloud security measures to protect hosted data and applications.²²

¹⁶ RBI/DPSS/2024-25/123

CO.DPSS.OVRST.No.S447/06-26-002/2024-25

¹⁷ Section 1 of Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators 2024.

¹⁸ Section III – Baseline Information Security Measures / Controls, Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators 2024

¹⁹ Point 19 of Section III – Baseline Information Security Measures / Controls, Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators 2024.

²⁰ Point 21(Patch and Change Management Life Cycle) of Section 3 of the Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators 2024.

²¹ Point 22 and 23 of the Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators 2024.

²² Point 24 and 26 of the Master Direction 2024.

The RBI's directions also provide detailed security protocols specifically for digital payment transactions, covering mobile payments, card transactions, and prepaid payment instruments.²³ Existing RBI guidelines for these payment types remain effective, but the new directions override any conflicting standards. Compliance deadlines vary by PSO size: large PSOs by April 1, 2025, medium PSOs by April 1, 2026, and small PSOs by April 1, 2028.²⁴ By mandating strong governance, updated security frameworks, and incident response protocols, these directions set a high benchmark for digital payment security. They aim to bolster customer trust and enhance the resilience of India's digital payment systems in the face of increasingly sophisticated cyber threats.

Framework on Alternative Authentication Mechanisms for Digital Payment Transactions

The Reserve Bank of India (RBI) has introduced a draft framework titled Alternative Authentication Mechanisms for Digital Payment Transactions²⁵, aiming to enhance security by strengthening the additional factor of authentication (AFA) requirements. Historically, SMS-based one-time passwords (OTP) have been the primary method for AFA in digital payment transactions involving cards, prepaid instruments, and mobile banking channels. However, technological advancements and the rise of new authentication options have led the RBI to explore alternative methods within a principle-based, flexible framework.

This framework is issued under Section 18 read with Section 10(2) of the Payment and Settlement Systems Act, 2007, this framework mandates all Payment System Providers and Participants, including both banks and non-banks, to adopt these alternative authentication mechanisms within three months from the issuance date. AFA is required for all digital payment transactions except certain cases, such as small-value, contactless card payments of up to ₹5,000 at point-of-sale terminals, recurring e-mandates, and low-value offline digital payments. For added security, the RBI specifies that AFA for non-card-present transactions must involve a dynamically generated factor—created post-payment initiation, unique to each transaction, and not reusable. An important aspect of the framework is customer protection. The RBI requires issuers to notify customers in real time for all eligible digital transactions, which provides an additional layer of security through customer awareness. Furthermore, issuers are prohibited from entering exclusive arrangements with any payment or technology service providers, thereby preserving flexibility in adopting diverse authentication solutions.

The RBI's draft framework for alternative authentication mechanisms aims to enhance digital payment security through diversified, risk-based AFA approaches while reducing dependency on SMS-based OTPs and fostering flexibility in adopting emerging technologies for robust digital transaction protection.²⁶

²³ Section 4 of the Master Direction 2024.

²⁴ Section 1 of the Master Direction 2024.

²⁵ CO.DPSS.POLC.No. S **/ 02-14-015 / 2024-2025, *available at*:

https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4477(last visited on 7 November 2024)

²⁶ Saloni Shukla, RBI issues draft framework on Alternative Authentication Mechanisms for Digital Payment Transactions, The Economic Times, *available at*: <https://economictimes.indiatimes.com/>

Aadhaar Enabled Payment System – Due Diligence of AePS Touchpoint Operators

The Reserve Bank of India (RBI) recently issued a draft framework on due diligence for Aadhaar Enabled Payment System (AePS) touchpoint operators²⁷, outlining key guidelines for onboarding, monitoring, and regulatory adherence. For the onboarding process, the draft mandates that acquiring banks must perform comprehensive due diligence on AePS touchpoint operators in line with the Customer Due Diligence requirements specified in the RBI's Know Your Customer (KYC) Directions, 2016. Additionally, if an AePS touchpoint operator remains inactive—meaning they conduct no financial transactions for six consecutive months—the acquiring bank must update the operator's KYC details before allowing any further transactions. Another critical directive is that AePS touchpoint operators should be onboarded by only one acquiring bank, a responsibility to be jointly managed by the National Payments Corporation of India (NPCI) and the acquiring banks.

The framework also emphasizes the importance of ongoing due diligence. Acquiring banks must continuously monitor AePS touchpoint operators, ensuring that their transaction limits align with their risk profiles and that their transactions are appropriate to their operational location. This ongoing surveillance helps prevent fraudulent or suspicious activities and ensures that operators act within the designated parameters based on their risk assessment. The draft reinforces that all System Participants involved in AePS operations must strictly adhere to NPCI's established rules and guidelines for AePS. This adherence ensures consistency and security in the functioning of AePS transactions across the network²⁸. By mandating these checks, the RBI aims to fortify the security and reliability of AePS touchpoints, bolstering trust and efficiency in Aadhaar-based digital payments.

Master Directions on Treatment of Wilful Defaulters and Large Defaulters

The RBI's Master Directions on Wilful Defaulters²⁹ are aimed at establishing a fair and consistent process for identifying borrowers who intentionally default on their loans, thereby protecting the stability of the financial system. These directions, issued under several legislative powers, including the RBI Act³⁰, the Banking Regulation Act³¹, and the Credit Information Companies Act³², are binding on banks and financial entities, making them enforceable in a legal context as well.

The revised guidelines provide a structured framework to address wilful defaults, upholding principles of transparency and natural justice. Created in response to growing concerns from the Central Vigilance Commission and parliamentary bodies, these directions have been shaped through extensive consultations to ensure fairness and effectiveness. Key elements include the classification of wilful defaulters and the handling of defaults, especially for amounts of INR

²⁷ CO.DPSS.POLC.No. S **/ 02-01-001 / 2024-2025, *available at*:

https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4475. (last visited on 7 November 2024)

²⁸ RBI releases draft rules for Aadhaar based payment operators to avert fraud, *available at*:

<https://www.business-standard.com/>(last visited on 7 November 2024)

²⁹ The Reserve Bank of India (RBI) has on July 30, 2024, issued the Master Directions on Wilful Defaulters and Large Defaulters (effective from October 28, 2024) (Master Circular/ Master Directions 2024),

³⁰ Section 45-L of the Reserve Bank of India Act, 1934

³¹ Section 21, Section 35-A and Section 35-A read with Section 56 of the Banking Regulation Act, 1949.

³² Section 11 of the Credit Information Companies (Regulation) Act, 2005.

25 lakhs and above. Quarterly reporting requirements by banks and financial institutions are mandated, with additional legal and criminal actions outlined for defaults of INR 1 crore and above.

This framework highlights wilful default as an intentional act that destabilizes the financial ecosystem, necessitating a clear understanding of obligations under laws like the Companies Act of 2013 and SEBI regulations. Both lenders and borrowers are required to adhere strictly to these standards, ensuring transparency and accountability. Through these directions, the RBI aims to enforce a proactive approach that safeguards the interests of all stakeholders in the financial sector, fostering compliance and deterring financial misconduct.

Framework for recognising Self-Regulatory Organisations for FinTech Sector

The Reserve Bank of India's (RBI) draft framework for recognizing Self-Regulatory Organizations in the fintech sector (SRO-FT)³³ outlines requirements to ensure that SROs promote innovation while protecting consumer interests.

Eligibility Requirements³⁴: To qualify, an SRO-FT applicant must be registered as a Section 8 company under the Companies Act, 2013, with an explicit mandate to operate as an SRO-FT in its Memorandum of Association (MoA). The applicant should also possess adequate financial resources and infrastructure, including IT systems, to manage reports of user harm. Additionally, any legal proceedings against the applicant or its leadership must be disclosed upfront, and the SRO-FT cannot operate overseas without prior RBI approval.

Membership Criteria³⁵: The SRO-FT should be inclusive of fintech firms of all types and sizes, including international members, with voluntary membership and a fair, non-discriminatory fee structure.

Application Process: Applications must include a detailed MoA and an operational plan. The RBI reserves the right to decide the number of SROs for each sub-sector and has the final say in granting recognition through a 'Letter of Recognition.' This recognition may be revoked if the SRO-FT's activities are found to be detrimental to the public or not aligned with its objectives.

Governance Framework³⁶: The SRO-FT is expected to uphold high standards of transparency, accountability, and compliance, while ensuring a conflict-free environment and addressing grievances promptly. It should have a professionally managed Board, with at least one-third of its members, including the chairperson, being independent and unaffiliated with any fintech entity.

The roles of Self-Regulatory Organizations (SROs) in the RBI's new framework and the Indian Banks' Association (IBA) are distinct yet complementary, with limited risk of overlap. SROs are tasked with enforcing compliance, setting industry standards, and fostering best practices across a range of financial institutions, including banks and NBFCs. In contrast, the IBA operates primarily as an advocacy body, representing banks in policy discussions with the government and regulatory agencies. While the IBA's focus is on policy advocacy and addressing industry-specific issues, SROs concentrate on regulatory oversight, ensuring adherence to RBI standards. This division of roles minimizes conflict; however, clear communication and defined responsibilities

³³ Draft Framework for Self-Regulatory Organisation(s) in the FinTech Sector, *available at*: <https://rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1260>. (last visited on 7 November 2024)

³⁴ Chapter 3 of the Draft Framework for Self-Regulatory Organisation(s) in the FinTech Sector.

³⁵ *Ibid.*

³⁶ Chapter 5 of the Draft Framework for Self-Regulatory Organisation(s) in the FinTech Sector.

among SROs, the IBA, and other industry bodies are essential to avoid redundancy and promote efficient, coordinated efforts across the financial sector.

Conclusion

The evolution of fintech in India has reshaped the financial landscape, introducing innovative solutions that enhance accessibility, efficiency, and financial inclusion. However, this rapid growth has underscored the need for comprehensive regulatory measures to mitigate potential risks. The Reserve Bank of India (RBI) has responded proactively by establishing a robust regulatory framework that balances the benefits of fintech innovation with the need for consumer protection and financial stability. The Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank payment system operators, for instance, represent a crucial step in fortifying the digital payment ecosystem against cyber threats. This is complemented by frameworks that provide alternative authentication mechanisms, enhancing security for digital transactions while accommodating the diverse user base in India. Additionally, the guidelines for Aadhaar-enabled Payment Systems (AePS) establish due diligence standards that ensure secure and reliable service delivery, especially in rural and underserved regions where Aadhaar-linked services are widely used. The RBI's emphasis on identifying and addressing willful and large defaulters through its Master Directions on defaulters reflects its commitment to fostering accountability and stability within the fintech and broader financial sectors. Furthermore, the RBI's recent draft framework for recognizing Self-Regulatory Organizations (SROs) in the fintech sector highlights its progressive approach to industry self-governance, allowing fintech companies to take an active role in compliance and best practices.

Despite India's significant progress in fintech, the sector faces critical challenges that could impede sustainable growth. One major gap is the limited financial literacy across much of the population, which can lead to misuse or misunderstanding of fintech products. Many users are unfamiliar with digital financial tools and may not fully comprehend risks associated with digital payments, loans, and investment platforms. The sector's rapid growth has also led to gaps in compliance infrastructure among fintech firms, especially smaller ones. These companies may lack the resources to maintain comprehensive regulatory and cybersecurity standards, increasing potential risks for consumers.

To bridge these gaps, financial literacy initiatives should be prioritized, helping consumers make informed decisions in the digital financial landscape. Targeted education campaigns can raise awareness of digital financial products, security practices, and consumer rights, particularly in rural and underserved regions. A strong partnership between fintech companies, regulatory bodies, and financial institutions can also facilitate shared oversight and self-regulation through Self-Regulatory Organizations (SROs), fostering a more resilient and inclusive fintech ecosystem in India.