Legal 500
Country Comparative Guides 2025

India
Fintech

Contributor

Shardul Amarchand
Mangaldas & Co

Shilpa Mankar Ahluwalia

Partner, Head- Fintech | shilpa.mankar@amsshardul.com

Himanshu Malhotra

Principal Associate | himanshu.malhotra@amsshardul.com

Purva Anand

Associate | purva.anand@amsshardul.com

This country-specific Q&A provides an overview of fintech laws and regulations applicable in India.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

India: Fintech

1. What are the regulators for fintech companies in your jurisdiction?

There is no umbrella regulatory framework governing the fintech ecosystem in India. The laws governing fintech in India are fragmented, with no single set of regulations or guidelines that uniformly apply to all fintech companies in India. The Reserve Bank of India (**RBI**), India's central bank, supervises most of the key verticals in the fintech space.

Other financial sector regulators, such as the Securities and Exchange Board of India (**SEBI**) and the Insurance Regulatory and Development Authority of India (**IRDAI**), act as supplementary regulators for fintech products which fall within their regulatory purview.

In addition to specific financial sector regulations, fintech companies must also comply with applicable know-your-customer (**KYC**) obligations, anti-money laundering (**AML**) obligations, and data privacy and protection requirements, which fall within the regulatory domain of specialised enforcement agencies. To strengthen self-regulation within the fintech ecosystem, the RBI has developed a framework for recognition of self-regulatory organisation(s) for fintech players in India (**SRO-FT**).

Set out below is an overview of the regulatory framework for fintech entities and the role of each regulator in India.

(a) RBI:

i. The Payment and Settlement Systems Act, 2007 (**PSS Act**) is India's principal legislation governing payment services. Under the PSS Act, no person can commence or operate a payment system in India without obtaining prior authorisation from RBI. The PSS Act defines a 'payment system' as "*a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service of all of them, but does not include a stock exchange*." Illustratively, payment systems under the PSS Act include systems enabling credit card operations, debit card operations, smart card operations, money transfer operations, and prepaid payment instruments (**PPIs**) (such as prepaid cards and mobile wallets) – bringing them all under the regulatory ambit of RBI.
ii. In its role as the principal regulator, the RBI also periodically issues master directions and circulars governing and regulating specific offerings in the fintech space. The RBI has issued subject-specific master directions and operating guidelines for regulating PPIs, non-banking financial companies (**NBFCs**), peer-to-peer lending platforms (**P2P Platforms**), payment aggregators and payment gateways (including cross border payment aggregators), payment banks, account aggregators, money transfer operators and other market participants and offerings.

(b) NPCI:

i. The National Payments Corporation of India (**NPCI**) is an umbrella, quasi-regulatory organisation for operating retail payments and settlement systems in India. NPCI is the not for profit implementing entity behind UPI, Aadhar enabled payment systems, Bharat bill payments system (through NPCI Bharat BillPay Limited), *RuPay cards* (a domestic cards system) and other payment systems and is registered with the RBI as an operator of payment systems under the PSS Act.
ii. The UPI payment system is primarily regulated by the UPI Procedural Guidelines, 2019, the UPI Operating and Settlement Guidelines and the circulars issued by the NPCI from time to time. They collectively govern transaction volumes, transaction caps, technical standards, data privacy and security measures, usage of UPI API, manner of settlement of transactions, etc. NPCI also issues guidelines and circulars governing the other retail payments and settlement systems under its ambit.
iii. NPCI has set up a dedicated wholly owned subsidiary, NPCI International Payments Limited (**NIPL**) which is aimed at building global payment networks linked to UPI and Rupay and to support. other nations in building their own real-time payment systems.

(c) IRDAI: IRDAI is the primary regulator in the insurance sector in India and supplements the regulatory framework of the RBI applicable to fintech players, specifically for InsurTech elements.

(d) SEBI: SEBI is the key financial markets regulator in India charged with the function of regulating the securities market and protecting investor interest. It has jurisdiction over aspects of fintech related to robo-

advisors, algorithmic trading and financial research platforms, although these areas are still nascent in India.

(e) FIU-Ind:

i. The Prevention of Money Laundering Act, 2002 read with the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (**PMLA Framework**) together are the primary legal framework for AML in India. The PMLA Framework imposes an obligation on financial sector entities, intermediaries and persons carrying on a designated business or profession to *first*, register with the Financial Intelligence Unit – India (**FIU-Ind**), and *second,* to verify identity of clients, maintain records, furnish information and report certain cash transactions and suspicious transactions to FIU-Ind.
ii. RBI's Master Directions on KYC dated February 25, 2016, require all regulated entities (**REs**) to abide by the provisions of the PMLA Framework and undertake identity verification of their customers before commencing any account-based relationship or as otherwise prescribed, and monitor their transactions. REs are also required to appoint a principal officer responsible for monitoring and reporting all transactions and sharing information as required under the law.

(f) UIDAI: Unique Identification Authority of India (**UIDAI**) is a statutory body responsible for administering Aadhaar. Aadhaar is a 12-digit unique identification number issued by the Government of India (**GOI**) to its citizens. UIDAI has been central to framing the rules governing the use of Aadhaar by fintech players as a means for customer onboarding and fulfilling KYC/AML compliances.

(g) Data Protection Board:

i. Data protection in India is currently governed by the Information Technology Act, 2000 read with the Information Technology (Reasonable Security Standards and Procedures and Sensitive Personal Data and Information) Rules, 2011 (**SPDI Rules**). While the SPDI Rules set out the broad guidelines applicable to processing and storage of customer data by service providers, they are not adequately equipped to address privacy issues and concerns created by modern day technological innovations in delivery and distribution of financial products and services.
ii. The GOI therefore enacted the Digital Personal Data Protection Act (**DPDP Act**) on August 11, 2023. The DPDP Act is a technology and sector agnostic umbrella framework that governs the processing of all digital personal data. The DPDP Act does not differentiate between the kinds of personal data and applies to the digital processing of data within India or in connection with goods and services offered in India. It outlines consent requirements, deemed consent principles, right of individuals to withdraw consent and request deletion of their personal data and the responsibilities of data fiduciaries and data processors while handling data. While the DPDP Act has been enacted, it is yet to be enforced. On January 03, 2025, the GOI released the draft Digital Personal Data Protection Rules, 2025 (**DPDP Rules**) for comments from the public and other stakeholders. The DPDP Act will come into force when the Government of India publishes notification(s) regarding commencement of the DPDP Act and the DPDP Rules in the official gazette. GOI will likely adopt a staggered approach to enforcement of the DPDP Act and the DPDP Rules. Upon effectiveness, the DPDP Act (read with the DPDP Rules) will replace the SPDI Rules to constitute the applicable statutory framework on data privacy and data protection in India.
iii. The DPDP Act provides for establishing a Data Protection Board of India (**DPB**), an independent body tasked with overseeing the implementation and enforcement of the DPDP Act. The DPB will be set up after the DPDP Act comes into force. Once established, the DPB will conduct inquiries based on complaints, address personal data breaches, issue directions and impose penalties for non-compliance.
iv. In addition, there are sectoral regulations which restrict the cross-border transfer of data or specify data storage in India for certain cases. The RBI's Circular on Storage of Payment System Data dated April 06, 2018 (read with clarifications issued by the RBI) (**Data Localisation Circular**) requires all banks and payment system operators to ensure that all data related to payments is stored only in servers located in India. Entities which are required to comply with the Data Localisation Circular are additionally responsible to contractually ensure that any intermediaries or other unregulated entities participating in payment transactions also comply with such localisation requirements. The RBI's Guidelines on Digital Lending dated September 02, 2022 (**DL Guidelines**) also require all data to be stored on Indian servers.

(h) SRO-FT: RBI has recently recognised the Fintech Association for Consumer Empowerment as the first SRO-FT. SRO-FTs can issue guidelines and best market practices which are binding on its members, supervise the operations of its members, take enforcement actions (including monetary penalties and reporting to the RBI) for any non-compliance, assist in resolving disputes and customer grievances and interact with the RBI for policy

level inputs. Indian fintech platforms have been nudged by the RBI to become members of the SRO-FT. By encouraging self-regulation, the RBI is permitting the fintech sector to proactively set and adhere to its own industry standards and best practices.

2. Do you foresee any imminent risks to the growth of the fintech market in your jurisdiction?

Frauds and unethical practices by unregulated entities pose the greatest risk underpinning growth of the fintech market in India. With increased usage of digital payment systems in India, there is a clear rise in the number and value of digital payment frauds against consumers. Digital payment frauds multiplied five folds year-on-year to INR 1,457 crores (~ USD 170 million) in FY 24 and formed 10.4% of the total fraudulent transaction value for FY 24 (as against 1.1% in FY 23). RBI is working with banks and enforcement agencies to strengthen transaction monitoring systems and ensure sharing of best practices for control of mule accounts and prevention of digital frauds. The RBIH is also piloting an artificial intelligence (**AI**) / machine learning (**ML**) based model, MuleHunter.AI, to address this concern.

Data security is another key concern. There have been instances of leaked Aadhar information being used for undertaking fraudulent payments. RBI (through its technology subsidiary) is setting up a secure cloud service for fintech players, to address the data security concerns at a systemic level. The RBI has been pro-actively monitoring compliance with IT security and privacy norms by financial entities regulated by it, and in a few cases, taken stringent actions for non-compliance with regulatory requirements. For instance, the RBI recently barred a major banking player from onboarding customers through digital channels and issuing new credit cards, citing a continued failure on part of the bank to address RBI's concerns regarding its IT systems. There have also been instances where RBI has prohibited REs from on-boarding new customers for non-compliance with data storage regulations.

India witnessed an unprecedented increase in enforcement actions by RBI against REs over the last year, primarily by way of monetary fines, penalties, and business restrictions. In exceptional cases, RBI has also revoked authorisations and licences granted to the defaulting REs.

RBI restricted an RE from onboarding new customers and from carrying on any further banking operations whatsoever (except customer withdrawals), due to their failure to comply with KYC/AML requirements. It also restricted four NBFCs from sanctioning or disbursing loans, for charging usurious interest rates from retail borrowers and other unfair lending practices. P2P Platforms also came under sharp regulatory scrutiny in 2024, with RBI expressing concerns on some business models where P2P Platforms performed quasi-lending and banking functions instead of acting as an intermediary.

Additionally, RBI imposed restrictions on certain lending products (secured and unsecured) offered by some NBFCs, expressing concerns over asset quality and credit underwriting standards. The RBI has also in the past revoked NBFC licenses of entities engaging in unfair lending practices, and aggressive recovery tactics which did not fulfil the regulatory criteria.

Industry players have expressed concerns about weakened market sentiment due to stringent regulatory actions taken by the RBI without much warning or an opportunity to engage before the action is put in place. The fintech sector is now beginning to contemplate a shift in focus from unsecured lending towards secured lending, even though this change involves higher costs associated with physical verifications and collateral checks.

3. Are fintechs required to be licensed or registered to operate in your jurisdiction?

The requirement of licensing/registration depends on the business model of the fintech platform.

For undertaking the business of banking in India or for undertaking financial activities as the principal business – fintech players require banking/ non-banking financial company licenses under the Banking Regulation Act, 1949 and Section 45I of the RBI Act, 1934. Fintech players which are operating a payment system or undertaking activities covered under the RBI's subject-specific master directions (an illustrative list provided in paragraph 1.4(a) above) will also require prior RBI authorisation.

Fintech players may also be required to obtain registrations with other financial sector regulators and other entities such as the FIU-Ind and NPCI, in addition to general compliance registrations applicable to all companies in India. For instance, WealthTechs which engage in securities broking and investment advisory services must register with SEBI, whereas InsurTechs such as insurance web aggregators, brokers and agents are required to be licensed by IRDAI.

Fintechs providing purely technology services, security

infrastructure or otherwise acting as service providers to REs in India, typically do not require registration with the RBI. The REs, which are directly regulated and supervised by the RBI, continue to be responsible with the regulations and also undertake responsibility for the actions of any unregulated entities they partner with. A standard industry practice is for regulatory risk and compliance requirements to be contractually passed on to unregulated entities, backed by suitable indemnity and termination of access provisions. In some cases, the RBI even specifies the contractual safeguards that an RE must build in, to ensure the regulatory compliance of the unregulated partner or service provider.

4. What is a Regulatory Sandbox and how does it benefit fintech start-ups in your jurisdiction?

The RBI has created a regulatory sandbox under the 'Enabling Framework for Regulatory Sandbox' dated August 13, 2019 (as updated from time to time) to allow testing of products and technology that are not currently governed by regulations and face some form of regulatory barrier in implementation, require certain regulatory relaxations for testing, and seek to improve delivery of financial services. The regulatory sandbox allows each stakeholder (regulator, innovators, the financial service providers and end users) to conduct pilots to collect evidence on the benefits of new financial innovations, while carefully monitoring and containing their risks.

Eligibility:

a. Eligible entities (including start-ups, banks, financial institutions, any other company, limited liability partnerships and partnership firms, partnering with or providing support to financial services businesses) can be selected for testing their products in the regulatory sandbox. The eligibility criteria include parameters such as: (i) net worth of at least INR 1 million, (ii) satisfactory credit score, (iii) promoters and directors of the applicant entity meeting the prescribed '*fit and proper*' criteria, (iv) ability to comply with personal data protection laws, and (v) adequate IT infrastructure and safeguards to protect against unauthorised access, alteration, destruction and disclosure. RBI's press release dated February 28, 2024, on the revision of the Enabling Framework for Regulatory Sandbox clarified that the REs within its regulatory sandbox framework must strictly adhere to the provisions of the DPDP Act.
b. The framework outlines the five stages of the sandbox process for a single cohort involving preliminary screening, finalising test designs, application assessment, closely monitored testing and lastly, assessment of the final output by the RBI. The end-to-end sandbox process practically takes more than 1.5 years for each cohort.

Successful cohorts:

a. The RBI contemplates product testing by a limited number of eligible entities in a single regulatory sandbox cohort (i.e., end to end sandbox process), where products broadly fall within a shared theme. As on date, the RBI has announced five cohorts — on retail payments (February 2021), cross border payments (December 2020), micro small medium enterprises lending (October 2021), prevention and mitigation of financial frauds (June 2022) and a fifth 'theme neutral' cohort.
b. Of these, the successful exit of 18 applicants from the first four cohorts has led to innovations such as a purely digital cash flow-based credit underwriting process for MSMEs, a voice-based UPI payment solution that supports local languages and offline use and an application which restricts any financial payments and login unless initiated using the credentials from the application making compromised financial passwords/cards useless for fraudsters.

IRDAI and SEBI: Similar to the regulatory sandbox implemented by the RBI for fintech products, IRDAI and SEBI have similar regulatory sandbox products in the InsurTech space, and for market-linked financial products offered by SEBI-regulated entities, respectively.

RBIH:

a. RBI has established a wholly owned subsidiary, the Reserve Bank Innovation Hub (**RBIH**) for ideation and development to promote innovation in the financial sector. The RBIH does not operate a regulatory sandbox. It instead acts as a research hub for developing digital public infrastructure products.
b. Notable examples united lending interface (**ULI**) and the FinTech and EmTech repositories. ULI is a technology platform built to facilitate easy access to authenticated data from various sources, through standardized application programming interfaces (**APIs**) to which all lenders can connect seamlessly through a 'plug and play' model. Colloquially dubbed the 'UPI of digital lending', ULI will enable frictionless credit and reduce costs by eliminating the need for lenders to integrate with diverse sources of financial and non-financial data such as government authorities, fintech players, techfin players, account aggregators, credit information companies and digital identity authorities. The pilot on ULI commenced from

August 17, 2023. As on December 06, 2024, loans amounting to INR 27,000 crores have been disbursed through ULI and thirty-six REs have been onboarded on ULI.

5. How do existing securities laws apply to initial coin offerings (ICOs) and other crypto assets, and what steps can companies take to ensure compliance in your jurisdiction?

Public reports on the Government of India's stance on regulation of crypto-assets indicate a shift from its earlier stance of a completely ban, to regulation of crypto assets and cryptocurrencies. While initial coin offerings (**ICOs**), cryptocurrencies and other crypto assets are *per se* not prohibited in India, their regulatory treatment is still a grey area except for the KYC/AML requirements applicable to service providers dealing with them. *Please refer to our response in paragraph 6 below.* ICOs are generally not viewed favourably by regulators in India given the number of several monetary scams involving cryptocurrencies and crypto assets.

Particularly on Indian securities laws – ICOs and crypto assets may not be classified as 'securities' under the Securities Contract Regulation Act, 1956 (**SCRA**) and currently are likely to not be recognized as such by SEBI.

While the definition of a security under SCRA is an inclusive definition, given the distinct and special nature of crypto currencies/assets, they might not necessarily meet the essential characteristics of a typical security such as shares, stocks, debentures and bonds. Securities typically are understood to be instruments which represent ownership or interest in the capital or debenture stock of an issuer and entitles the holder to exercise voting and/ or economic rights against the issuer, on account of holding such securities. It can be argued that crypto currencies/assets typically do not represent a share or a unit of any incorporated company or a pooled investment vehicle or any other body corporate. Further, their value is determined largely by the market forces of demand and supply and is not linked to the performance of any underlying issuer.

The regulation of ICOs, crypto currency and crypto assets in India remains unclear and is evolving. GOI has set up a panel to propose a regulatory policy for crypto assets in India. Basis publicly available information, SEBI has in its recommendations to the panel stated it was open to monitoring cryptocurrencies that take the form of securities as well as new offerings (ICOs).

6. What are the key anti-money laundering (AML) and Know Your Customer (KYC) requirements for cryptocurrency exchanges in your jurisdiction, and how can companies implement effective compliance programs to meet these obligations?

Indian regulators have focused on regulating crypto intermediaries (including cryptocurrency exchanges) with rules centred around KYC requirements, consumer protection, disclosures and reporting requirements.

GOI issued a notification on March 07, 2023 (**VASP Notification**), terming virtual asset service providers as 'reporting entities' under the PMLA Framework. Under the VASP Notification, virtual asset service providers include entities carrying on, in the course of business and on behalf of another person, the exchange between virtual digital assets and fiat currencies or between one or more forms of virtual digital assets – and will squarely include cryptocurrency exchanges within its ambit. FIU-Ind has also published on its website a set of guidelines known as the 'AML & CFT Guidelines for Reporting Entities Providing Services Related To Virtual Digital Assets' (**FIU-Ind Guidelines**) with effect from March 10, 2023.

Consequently, every cryptocurrency exchange operating in India needs to: (a) register with the FIU-Ind, (b) adopt the prescribed KYC verification processes to verify the identity of users at the time of onboarding and (c) comply with other obligations under the PMLA Framework (such as maintaining transaction records for the time period specified under the PMLA Framework, reporting of suspicious transactions and specified transactions to the FIU-Ind).

Particularly on KYC compliances, cryptocurrency exchanges will need to have in place effective procedures to properly identify customers and take the prescribed measures to identify and verify the beneficial owners. The cryptocurrency exchange must also upload an electronic copy of the customer's KYC records with CERSAI (the central KYC registry) within 10 days of onboarding/ commencement of an account-based relationship with the customer. The cryptocurrency exchange must also carry out periodic KYC updates, in accordance with the risk-based assessments carried out by the cryptocurrency exchange. The FIU-Ind Guidelines also prescribe enhanced due diligence norms for complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose and for transactions involving high-risk jurisdictions or persons.

The FIU-Ind has been actively enforcing the FIU-Ind

Guidelines. In the past, it has issued show cause notices to several cryptocurrency exchanges for failing to obtain registration and directed GOI to block their URLs.

To meet these obligations, cryptocurrency exchanges can implement several strategies including developing comprehensive compliance policies which are regularly updated to reflect changes in regulations, investing in technology solutions and engaging third party audits for assessing any shortfalls in compliance.

7. How do government regulations requiring licensing or regulatory oversight impact the operations of cryptocurrency and blockchain companies in your jurisdiction, and what strategies can be employed to navigate these varying requirements?

Please refer to our response in paragraphs 5.1 and 6 above. The regulatory treatment of cryptocurrency in India is a grey area, except for the KYC/AML requirements applicable to service providers dealing with them. While not prohibited *per se*, cryptocurrencies are not viewed favourably by financial regulators in India.

In contrast to their approach towards cryptocurrency, GOI and regulators have a positive approach to blockchain technology. The GOI has encouraged adoption of blockchain technology to streamline maintenance of public records such as land records, title documents and KYC information.

8. What measures should cryptocurrency companies take to comply with the governmental guidelines on tax reporting and obligations related to digital assets in your jurisdiction?

The Indian direct tax laws require the person responsible for paying any resident any sum as consideration for the transfer of a virtual digital asset (including cryptocurrencies) to deduct 1% of such sum as income tax. In cases where the transfer involves multiple parties such as the crypto exchange, brokers (apart the actual purchasers and sellers), the tax department has issued a circular clarifying the person(s) responsible for deducting these taxes. The circular also provides guidance on the manner of income tax deduction in cases involving cryptocurrency exchanges. Consequently, the relevant cryptocurrency company (acting as a broker, exchange, buyer or seller) must evaluate their tax withholding obligations and undertake requisite reporting compliances, if any.

Any cryptocurrency exchange set up in India would need to comply with appropriate Goods and Service Tax (**GST**) compliances for services rendered to Indian residents. The exchange would be required to take an appropriate GST registration in each state of operation. This involves, among others, having a running principal place of business in the state, an Indian bank account and an authorized signatory residing in such state for the purpose of compliance. Thereafter, the exchange will be required to the monthly and annual GST returns. The exchange may have a GST liability on commission income earned from transactions on the platform, among other liabilities, as may be applicable. The GST rate would be 18% for such services. The exchange can take input tax credit of GST paid on input goods and services received (as applicable) to offset the output GST liability, subject to compliance of appropriate requirements under GST laws. Currently, there is no domestic cryptocurrency exchange in India.

If an offshore cryptocurrency exchange is providing services to GST registered service recipients with the place of supply as India, the liability for GST compliance is on the Indian service recipient. The question on whether there is an obligation on an offshore cryptocurrency exchange to obtain registration and deposit GST when the service recipient is not registered for GST in India is currently unsettled. Indian authorities allege that cryptocurrency exchanges provide online information database and retrieval services and are therefore required to register and pay GST in India, whereas the overseas exchanges and the cryptocurrency industry have challenged the same arguing that they are at the most intermediaries with their place of supply of services (as per GST laws) outside India, and therefore they do not fall under the ambit of GST laws in India. This issue of jurisdiction of GST laws (for overseas exchanges) is currently sub judice in various high courts in the country.

9. How can blockchain companies address data privacy and protection regulations in your jurisdiction, while ensuring transparency and security on decentralized networks?

For an overview of the applicable statutory framework on data privacy and data protection in India – *please refer to our response in paragraphs 1.4(g) (i) and (ii) above.*

There are certain design conflicts between the nature of blockchain technology and the data privacy frameworks under the SPDI Rules and the DPDP Act. For example:

a. Blockchains can, by design, be fundamentally

immutable. Whereas, Section 8(7) of the DPDP Act requires a data fiduciary to delete, and cause any data processors to delete, the personal data of a person once they withdraw consent or when the purpose for which consent was provided is no longer being served, unless retention is necessary for compliance with any law. Blockchain immutability presents a significant challenge in ensuring compliance with the right of erasure.

b. The lack of a clear data controller or processor in decentralized networks complicates accountability under SPDI Rules and the DPDP Act.
c. Depending on the nature of business operations of the blockchain company, certain sectoral regulators may require data to be stored only within India. *Please refer to our response in paragraphs 1.4(g)(iv) above.* Further, Rule 7 of the SPDI Rules and Section 16 of the DPDP Act may restrict cross-border data transfers to certain jurisdictions. However, blockchain's decentralised and globally accessible nature makes it challenging to enforce such restrictions.

To effectively address these challenges while ensuring transparency and security, blockchain companies can implement several strategies, including (a) utilizing permissioned blockchains which can control access to data; (b) implement technological solutions such as zero-knowledge proofs which enable verification of information without revealing actual data; (c) encrypt or anonymise data before it enters the blockchain to make it inaccessible or so that it is no longer personal data (which can be used to identify individuals); (d) utilising off-chain storage solutions to facilitate compliance with deletion requests; and (e) conducting data protection impact assessments / third party audits to identify potential risks associated with data processing activities on blockchain networks and to identify potential shortfalls in compliance with the SPDI Rules and the DPDP Act.

10. How do immigration policies, such as the U.S.'s H-1B and L-1 visas, impact the ability of fintech companies to hire international talent in your jurisdiction?

There is no quota system in place for any sector for foreign nationals entering India. However, as per the guidelines issued by the Bureau of Immigration, Ministry of Home Affairs, a foreign national being sponsored for an employment visa in any sector should draw a gross salary in excess of USD 25,000 per annum. Further, as per the employment visa requirements, employment visa is not granted for jobs for which qualified Indians are available or for routine, ordinary, secretarial or clerical jobs. It is granted to highly skilled/ qualified professionals or to persons engaged or appointed on contractual or employment basis. Consular and immigration officials consider an applicant's academic and professional qualifications to fill the proposed position in India, and the availability of Indian workers to fill the position.

Typically, employment visas for most sectors are processed on a case-by-case basis and are granted for one year even if the duration of employment is longer than a year and it is possible to get an extension of the visa in India for an additional twelve-month period, enabling the individual to remain in India on the employment visa for up to a total of five years from the date of initial issue of the visa. The extension procedure and processing time differs in every jurisdiction within India. Special provisions regarding visa duration, processes and validity apply to the citizens of certain jurisdictions.

There has generally not been a concern among global fintech platforms regarding their ability to hire international talent for their operations in India.

11. What are the key regulatory and compliance requirements that a fintech must address when entering the market in your jurisdiction, and how can the company ensure adherence to all applicable laws and regulations?

The laws governing fintech companies in India are fragmented. *First,* fintech players must comply with regulations issued by RBI, SEBI and other financial sector regulators (including any data localisation requirements); KYC/AML requirements; and data privacy legislations (the SPDI Rules and the DPDP Act). For an overview of these regulatory requirements in India, *please refer to our response in paragraph 1 above.*

Second, under foreign exchange laws in India, a foreign company can only undertake business activities in India through a place of business established in accordance with the Companies Act, 2013 and the Foreign Exchange Management (Establishment in India or a branch office or a liaison office or a project office or any other place of business) Regulations, 2016. Pursuant to the Consolidated Foreign Direct Investment Policy of India, 2017 (**FDI Policy**) and the Press Note No. 3 (2020 Series) (**PN3**), depending on the nature of business and the country of origin of the foreign investment or the beneficial owner of the foreign investment (whether it is a country sharing land border with India), fintech players

may be subject to restrictions on the maximum permissible foreign investment and need government approvals for foreign investment beyond such limits.

Third, upon establishing such an entity in India, fintech companies must also adhere to the compliance requirements applicable to companies/businesses generally in India. The Companies Act, 2013 (**Companies Act**) governs the incorporation, management, and operation of companies in India. Fintech players will also be required to comply with applicable labour laws. Some of the important legislations which require registration by companies are state-specific shops and establishments, the Employees' Provident Funds and Miscellaneous Provisions Act, 1952, the Employees' State Insurance Act, 1948, and Payment of Gratuity Act, 1972. Compliance with tax laws is another key area. Foreign fintech players having set up a permanent establishment in India must obtain tax registrations in India and ensure compliance with direct and indirect tax filings. *Please refer to our response in paragraph 8 above.*

Fintech entities can utilise integrated RegTech solutions to ensure compliance, monitoring, reporting, and managing regulatory requirements in real time. RegTech solutions offer functionalities like automated KYC verification / AML screening, data protection management, and tax compliance, which reduce the risk of errors, enhance operational efficiency, and ensure continuous alignment with regulatory updates.

12. How should a fintech approach market entry strategy in your jurisdiction, considering factors such as target customer demographics, competitive landscape, and potential partnerships with banking and other financial institutions?

Fintech players looking to enter the Indian market must have tailored customer acquisition strategies and efficient management of local partnerships with REs.

Indian is the third largest and the fastest growing fintech market globally. India's fintech market is expected to reach USD 150 billion by 2025, a threefold increase from USD 50 billion in 2021. Indians are also the most open to adopting fintech solutions. Indians have a fintech adoption rate of 87% (against a global average of 64%). The digital payments index (a statistic published by the RBI to capture the extent of digitization of payments) saw a 12.6% year on year increase as of March 31, 2024. India is also expected to have about 900 million plus active internet users with one of the cheapest internet accesses globally (1 GB of internet in India costs about USD 0.16). Digital public infrastructure is at the core of this acceptance of financial technology, with the India Stack, increasing internet penetration and favourable demography being the key enablers.

On the flip side, India has an extremely diverse and fragmented demographic, with nuances on local preferences that the fintech players must account for while breaking into the market. Additionally, fintech players looking to tap into the Indian market not only face competition from the REs and other new-age fintech startups, but also need to constantly adapt with India's digital public infrastructure model and regulatory developments.

Banks and non-bank fintech players had initially launched competing products and the fintech landscape in India was, for a while, segmented into bank vs. non-bank players. However, the market has now shifted to a more collaborative model, with banks and non-bank entities partnering on several dimensions, each leveraging their respective strengths, to provide customers easy to use financial products. Non-banks are not burdened by legacy systems and processes and can adopt emerging technologies to anticipate and satisfy customer needs, while accessing customers and markets that banks would find too expensive to tap in the ordinary course. Banks have strong balance sheets and a robust understanding of the regulatory and licensing regime governing financial products.

Partnerships between fintech platforms and REs are a regular occurrence for virtually every product segment. In the payments landscape, banks regularly partner with third party technology service providers to manage the customer and product interface for both PPI and UPI based payment products. In the digital lending space, traditional lenders such as NBFCs are increasingly collaborating with fintech platforms to act as Lending Service Providers (**LSP**) and Digital Lending Applications (**DLA**). Further, acceleration of account aggregator adoption by the ecosystem and expanding to other data sources beyond banks will unlock financial industry's ability to drive better access, undertake algorithmic risk-based lending through open market platforms and offering tailor made financial products to their customers.

13. What are the primary financial and operational risks associated with entering the market in your jurisdiction, and how can the fintech effectively mitigate these risks to ensure

a smooth transition and sustainable growth?

The master directions and circulars issued by the RBI for regulating specific offerings in the fintech space specify a minimum positive net worth. For instance, entities must have a minimum positive net worth of INR 50 million to apply to the RBI for an authorisation to issue PPIs and must achieve a minimum positive net worth of INR 150 million, by the end of the third financial year from the date of receiving final authorisation from the RBI, which must be maintained thereafter on an on-going basis. Similarly, a payment aggregator (**PA**) in India must comply with the minimum positive net worth of INR 150 million at the time of application to the RBI and must achieve a minimum positive net worth of INR 250 million after the end of the third complete financial year from the final approval, which must be maintained at all times, on an on-going basis. These minimum capital requirements to be maintained on an ongoing basis establishes stability of fintech entities enabling payments in India but requires an upfront capital commitment.

Regulatory risk is another significant concern for fintech players that are REs, given the increased enforcement actions by RBI over the last year. Recent enforcement actions have highlighted the business continuity risks fintech players face when regulatory gaps emerge. Even for non-RE fintech players, there is a risk of such enforcement action placing restrictions on its partner RE which restricts business functions. Further, as the Indian fintech sector evolves, regulatory frameworks (including those from the RBI), continue to develop. Fintech players often find themselves adapting to these emerging regulations and may need to respond swiftly to stay compliant. Accordingly, fintech entities need to anticipate and prepare for any impact of future regulations on its business models. Fintech entities must also accordingly design flexible business models that can absorb regulatory shifts, ensuring sustained operations and long-term market credibility.

The operational risks for fintech entities in India include: (a) challenges in managing customer data securely, (b) navigating the nuances of local consumer behaviour given India's diverse demographics, (c) strong competition in the fintech startup ecosystem in India, (d) the need to constantly adapt with India's digital public infrastructure model and regulatory developments, and (e) ensuring scalability of tech infrastructure.

To effectively mitigate financial risks, fintech entities can undertake proactive regulatory engagements (for instance through RBI's periodical 'finteract and finquiry' sessions), and undertake regular consultations with legal experts for understanding evolving regulations and adapting business models accordingly. Fintech players must also develop a comprehensive risk management plan that includes regular risk assessments, clear policies for credit control, investment management, and internal controls.

Investing in robust cybersecurity measures to protect customer data and developing scalable, adaptable platforms can address the above operational risks. A clear strategy for customer education and local market adaptation is also essential for sustainable growth and risk reduction.

14. Does your jurisdiction allow certain business functions to be outsourced to an offshore location?

Yes, REs and fintech platforms in India can outsource certain business functions offshore.

Outsourcing of financial and information technology services by banks and NBFCs is currently governed by separate guidelines/directions issued by the RBI. Notably, the RBI restricts REs from outsourcing core management functions, including internal audits, compliance, and decision-making functions (like determining KYC compliance for opening accounts and sanctioning loans), with some relaxations for group companies.

Any outsourcing of such regulated business functions by an RE typically requires that the RE have a board-approved policy for such outsourcing and a robust grievance redressal mechanism. The RE must conduct due diligence on its service providers, continue to monitor and control the outsourced activity and ensure confidentiality of its customer data. Such outsourcing will also attract reporting and risk management obligations on the RE. RBI also prescribes the form and contents of the outsourcing agreement between the RE and the service provider.

RBI also specifies additional requirements for cross-border outsourcing.

Typically, REs need to closely monitor government policies and the political, social, economic and legal conditions of the jurisdiction in which its service providers are based (on a continuous basis) and must have appropriate contingency and exit strategies in case of any adverse development. The outsourcing arrangement must specify the governing law upfront. The RE, in principle, must not enter into outsourcing arrangements with service providers operating in jurisdictions that do not uphold contractual

confidentiality obligations. Further, the right of the RE and the RBI to direct and conduct an audit or inspection of the service provider based in a foreign jurisdiction also needs to be protected. The RE will also need to comply with restrictions on data storage, sharing, and maintenance of records.

As a thumb rule for any outsourcing – the RE/ fintech players must assess and ensure that such offshore outsourcing arrangement neither diminishes its ability to fulfil its obligations to customers and the RBI nor impedes adequate supervision by the RBI.

15. What strategies can fintech companies use to effectively protect their proprietary algorithms and software in your jurisdiction, and how does patent eligibility apply to fintech innovations?

Under Indian law, software codes and computer programs (through underlying codes) (including AI products) are automatically protected by copyright as 'literary work' under the Copyrights Act, 1957. Brands, logos, sounds, colours and 3D shapes are protected by the Trademarks Act, 1999 (**Trademarks Act**). Design protection can keep a product's distinctive visual components protected.

Innovative fintech products can be protected under Patents Act, 1970 and the Copyrights Act, 1957. Companies have in the past filed patent applications with the patent office in India for patenting blockchain based technology that provides financial solutions. Software/computer programs *per se*, algorithms or business methods are not patentable subject matters. However, when the software/ computer program is tied to a physical invention or hardware (i.e. when it is a component of the invention) and where it demonstrates a technical effect or technical contribution, it may be granted patent protection. To be patentable, an invention must incorporate a non-obvious inventive step that is technically advanced or economically significant and is capable of industrial application.

16. How can a fintech company safeguard its trademarks and service marks to protect its brand identity in your jurisdiction?

Under the Trademarks Act, both civil and criminal remedies are available against infringement and passing off. Registration of a trademark is not a prerequisite in order to sustain a civil or criminal action against violation of trademarks in India.

Trademark owners can seek various reliefs, including temporary or permanent injunctions, damages, and orders for the destruction of infringing materials. Interim injunctions can be granted *ex parte* or after notice.

The Trademarks Act outlines criminal penalties, including imprisonment and/or fines, for falsification of trademarks (making a trademark without its proprietor's assent), applying falsified trademarks or selling or possessing goods having falsely applied trademarks.

17. What are the legal implications of using open-source software in fintech products in your jurisdiction, and how can companies ensure compliance with open-source licensing agreements?

Open source software (**OSS**) refers to a software licensing model that allows users to access the source code of the software royalty-free, under terms that permit redistribution, modification, and enhancement, albeit often with specific restrictions. This model represents a significant departure from traditional proprietary software rights.

For a fintech entity (or any entity) utilizing OSS, adherence to licensing agreements is crucial. Broadly, OSS licenses are of two types:

a. **Copyleft licenses**: Licenses that protect the copyright or patent of the OSS while allowing users to use, modify, and distribute the software with a condition that any modifications made must be shared back with the community under the same licensing terms. (That is OSS licenses with a reciprocal obligation to contribute improvements as OSS.)
b. **Permissive licenses**: Licenses that allow users to modify and redistribute the software without requiring derivative works to be open source. (That is OSS licenses that permit the creation of proprietary derivatives from the OSS.)

Fintech entities using OSS undertake the risk of liability for copyright and patent infringements if the licensing terms are not complied with. Thus, fintech entities using OSS for developing their proprietary products must identify all OSS being so utilized, review their licensing terms and ensure that they have permissive licensing arrangements, assess associated risks and obligations and establish a robust compliance mechanism to manage these risks effectively. Such compliance mechanisms can include regular comprehensive audits for software components, maintaining an inventory of all OSS components utilized in their proprietary products

and by addressing OSS explicitly in contractual relationships.

If the fintech entity is the consumer of a proprietary product – in addition to umbrella warranties for compliances with applicable law and previous contractual arrangements by the vendor – the fintech entity can require its contracts to contain specific warranties that no OSS was utilised, or alternatively request for details of all OSS utilised and a warranty that the vendor has complied with the licensing terms of the OSS. On the flip side, if the fintech entity is the vendor of a proprietary product, it may seek disclaimers of warranties regarding OSS implications. Inclusion of standard intellectual property (**IP**) indemnity clauses in such contracts is also a critical consideration.

18. How can fintech startups navigate the complexities of intellectual property ownership when collaborating with third-party developers or entering into partnerships?

It is recommended that fintech players fully address ownership of IP contractually, especially for IP developed through collaborations with third-party developers or through partnerships. Corresponding representations and warranties, indemnities and disclaimers must be included in the contractual arrangements executed for such collaborations.

Unless contractually provided otherwise, the ownership of any IP developed by a third-party developer will typically remain with the developer (i.e., the inventor / the author). The ownership of IP developed through collaborative partnerships may become a factual determination (taking into account the artistic and technical contributions of each person, extent of collaborations, who developed the inventive step etc.) and may lead to commercially undesirable outcomes (such as a joint ownership over the IP which may not be commercially valuable to either person individually).

As a step further, fintech players can also enter into non-disclosure and confidentiality agreements to protect their proprietary information and/or IP while exploring and entering into collaborations or partnerships with any third parties.

19. What steps should fintech companies take to prevent and address potential IP infringements, such as unauthorized use of their technology or brand by competitors?

Statutory enforcement rights offer the strongest enforcement mechanisms for IP infringements. Although it is not a prerequisite for enforcement actions, fintech entities must endeavour to register their IP as it offers *prima facie* evidence of ownership in case of any disputes.

Statutory remedies for IP infringements include both civil and criminal remedies. Civil suits before courts and/or alternative dispute redressal are the typical mechanisms for enforcement actions against an infringer. The reliefs include fines, temporary or permanent injunctions, damages or account of profits, and orders for the destruction of infringing materials/goods. Statutory penalties in India also include imprisonment for up to three years.

If a company's or an individual's IP rights are infringed, such a person may file a civil suit for infringement before the courts. When an IP right is infringed upon, the owner of the right can apply to the courts for an injunction (restraining the person from using the IP), an account of profits, damages and the destruction of goods.

Other than statutory remedies, enforcement actions can also be taken based on common law rights that are available in India. For example, common law rights for trademarks in India can arise from local use of the mark or from spill-over reputation.

20. What are the legal obligations of fintechs regarding the transparency and fairness of AI algorithms, especially in credit scoring and lending decisions? How can companies demonstrate that their AI systems do not result in biased or discriminatory outcomes?

Fintech companies must comply with the regulatory requirements of transparency and fairness in India, including when they utilize AI products/algorithms, particularly in credit scoring and lending decisions. According to RBI's 'Master Circular- Loans and Advances – Statutory and Other Restrictions' from July 1, 2015, REs are prohibited from discriminating basis sex, caste, or religion while making any lending decisions. Any AI tools or algorithms employed in lending decisions or in credit scoring must comply with this directive.

Further, the DL Guidelines (which establish a regulatory framework for digital lending in India) focus on three core principles: transparency, auditability, and relevancy in the

parameters utilized for credit scoring and lending decisions.

The DL Guidelines require REs to capture a detailed economic profile of borrowers, including aspects such as age, occupation, and income, before extending loans through their DLAs or in partnership with LSPs. This creditworthiness analysis must be conducted fairly and in a manner which can be audited. Further, any data collected by LSPs or DLAs must be only with the prior explicit consent of borrowers, complete with an audit trail. The rationale for collecting data must also be transparently communicated at each stage of interaction.

To comply with these requirements, REs and LSPs employing AI solutions for lending decisions must ensure that the data collected is strictly used for the purposes disclosed to the borrower, thereby maintaining transparency. Additionally, there must be a verifiable record for the technological applications used, the rationale behind credit decisions, and evidence of borrower consent for data collection, thereby ensuring auditability. Furthermore, REs must ensure that there is a clear and demonstrable connection between the data collected and the borrower's economic profile, ensuring that the data collection is justified within the context of the credit decision-making process.

To mitigate potential biases in AI algorithms and to comply with the auditability requirements specified above, fintech players can implement algorithmic explainability and avoid blackbox AI models. To this end, fintech players must make adequate and relevant disclosures about how AI systems are being used to make decisions, what data is being used to train AI systems, and address other forms of information asymmetry, allowing users and auditors to understand and contest lending decisions if necessary. Incorporating manual oversight and intervention is also crucial. This element of a 'human application of mind' will allow for the identification and rectification of any discriminatory outcomes, thereby addressing both algorithmic and procedural biases. Implementing regular internal reviews and third-party audits of the AI products and algorithms to identify and address issues of fairness, accountability, and transparency is also advisable.

21. What are the IP considerations for fintech companies developing proprietary AI models? How can they protect their AI technologies and data sets from infringement, and what are the implications of using third-party AI tools?

Proprietary AI models are protected by copyright in India and may be protected by patents. *Please refer to our response in paragraph 15 above.* Fintech entities should formalize IP ownership through detailed contracts, ensuring that rights over developed AI models and datasets are clearly defined, especially in collaborative projects or where data originates from multiple sources. *Please refer to our response in paragraph 18 above.*

To protect developed AI models and datasets from infringement, fintech entities can implement multi-layered strategies including trade secret protections, NDAs, and technical safeguards like encryption and access controls. Registering trademarks for AI-products and maintaining detailed records of AI model development can further establish ownership. For datasets, anonymization and data licensing agreements are crucial to prevent and mitigate liability in case of any unauthorized access or use. Further, in the event of any IP infringement, fintech entities are protected both statutorily and through common law remedies. *Please refer to our response in paragraph 19 above.*

Using third-party AI tools presents additional risks, including unclear IP ownership, dependency on proprietary algorithms, liability for IP infringement (for instance if the AI model was trained by protected materials, by infringing another's IP), and data privacy concerns. Fintech entities must thoroughly review licensing agreements to ensure clarity on data rights, usage of any OSS, limitations on derivative works, and indemnity clauses against IP. *Our response in paragraphs 17.3 and 17.4 above touches upon these aspects.*

22. What specific financial regulations must fintechs adhere to when deploying AI solutions, and how can they ensure their AI applications comply with existing financial laws and regulations? Are there specific frameworks or guidelines provided by financial regulatory bodies regarding AI?

While there are currently no comprehensive regulations specifically addressing AI in India, the financial sector regulators RBI and SEBI have initiated steps to address the adoption of AI in existing financial regulations.

In its Statement on Developmental and Regulatory Policies issued on December 6, 2024, the RBI announced the formation of an eight-member committee to develop a 'Framework for Responsible and Ethical Enablement of AI' (**FREE-AI**) to recommend a robust, comprehensive, and adaptable AI framework for the financial sector.

In 2019, SEBI issued circulars aimed at ensuring transparency, accountability, and regulatory oversight in the use of AI/ML technologies across different financial market participants. These circulars mandate entities, which are utilizing AI and ML technologies, to submit quarterly reports to SEBI in the prescribed format within 15 days from the end of each quarter. These reports detail the specific technologies employed, the safeguards implemented to prevent abnormal behavior of AI systems, and other relevant information.

Recently, SEBI issued a consultation paper on November 13, 2024, targeting the governance of AI/ML technologies in financial markets. This proposal extends SEBI's systematic approach of tracking AI/ML applications across various market participants since 2019. SEBI has defined 'artificial intelligence tools' as including software programs, executable systems, or a combination used by stock exchanges, clearing corporations, or internally within entities for trading, settlement, compliance, or other business activities, whether offered to investors or used internally.

The consultation paper proposes amendments such that entities deploying AI tools, whether developed in-house or procured from third parties, will be: (a) accountable for data integrity, ensuring the privacy, security, and integrity of investor and stakeholder data, including fiduciary information; (b) responsible for AI outcomes, including bearing liability for the consequences of decisions or actions resulting from AI outputs; and (c) ensure adherence with all applicable laws while using AI.

For any violations, SEBI retains the authority to take enforcement action, including penalties or other measures. The amendments emphasize the need for robust safeguards and responsible AI usage. The consultation paper also suggests using proportionate measures for small and medium-sized entities, acknowledging that compliance must be scalable and ensuring smaller firms can adopt AI responsibly without undue burden.

23. What risk management strategies should fintech companies adopt to mitigate potential legal liabilities associated with AI technologies?

While adoption of AI tools continues to contribute significantly to the growth of the fintech sector in India, there are risks associated with increasing adoption of AI technology. Use of AI utilities involves access to sensitive customer data including inter alia financial information, credit history, spending patterns, etc. Financial service providers must comply with the changing regulatory landscape in respect of data privacy and digital lending in India to ensure an uninterrupted use of AI in financial services. Adoption of a robust data governance framework, which includes data encryption, secure access controls, and clear data usage policies is critical with increasing reliance on AI tools by fintech players.

In addition, while deploying AI in high-value decision making use cases, financial service providers must also be mindful of any potential adverse impacts. 'AI biases' can arise from limited training data/ faulty considerations, which could further perpetrate social inequities. Thus, in decision making use cases, financial service providers must ensure close human supervision and an auditable decision making criteria. *Please see paragraph 20 above, particularly the recommendations in paragraph 20.5 above*. Additionally, creating clear terms of use, disclaimers, and ensuring consumer consent for automated decision-making processes can mitigate potential legal risks and customer grievances.

24. Are there any strong examples of disruption through fintech in your jurisdiction?

While India has traditionally been a cash-based economy, it is now rapidly transforming into a digital economy on the strength of the digital payment products offered by fintech players operating in the country. UPI has been the strongest disruptor of the payments landscape in India. TPAPs operating within the UPI ecosystem have effectively disrupted peer to peer and peer to merchant payments in India. Introduction of credit on UPI has further multiplied access and acceptance of credit cards through the UPI infrastructure.

Notably, in 2025, NPCI's products such as UPI123Pay and Hello!UPI – which enable instant payments for users with feature phones, with limited or no internet connectivity or through voice-enabled payment instructions in a regional language – are set to disrupt how the traditionally underserved rural India makes its payments.

UPI Global is also poised to significantly disrupt cross border payments to and from India. For countries with developed payment systems or with large remittances to India, NIPL creates bilateral linkages between UPI and the payment systems locally available to reduce the cost of remittances (for e.g. the UPI – PayNow linkage with Singapore). NIPL also assists countries in developing their own UPI-like payments systems (for e.g. Nepal). NIPL is also partnering with central banks, local and international digital payment service providers and PGs to enable international merchant payments (typically using QR code interoperability) (for e.g. NIPL has

partnered with Liquid Group, Lyra, Neopay, Worldline, Central Bank of Oman and PPRO). Cross-border payments are currently dominated by the Visa-Mastercard UPI has significant advantages over the incumbent card networks with its secure and user-friendly interface, reduced costs and real-time transactions. Nevertheless, UPI Global is still in its nascent stage and will take a few years to play out.

Apart from the payments sector, fintech players are now creating disruptions in the lending and investments space. Rapid disruption in unsecured lending has improved customer experience, encouraged analytics-based credit decisioning and reduced costs of service and customer acquisition. A one-time integration with the ULI platform will eliminate the need for lenders to carry out multiple bilateral integrations with each data and service provider, facilitating frictionless credit. Fintech players have also disrupted the investments and money management space, enabling mobile based investments into securities, mutual funds and even cryptocurrency investments. Key enablers include an online and seamless KYC process, easy fee collection, and providing access to account aggregator ecosystem, with market wide depositories information access. A similar tech-enabled disruption to improve customer access and experience is also taking place in the InsurTech space.

Additionally, further disruption in the payments ecosystem is expected due to adoption of evolving technologies such as block-chain and AI by payment service providers. Both bank and non-bank entities have already began to rely on AI based tools to improve customer experience, especially, in the areas of product identification and matching, background and credit verification checks which all make for a seamless customer experience.

25. Which areas of fintech are attracting investment in your jurisdiction, and at what level (Series A, Series B, etc.)?

Digital lending has attracted most funding in the last three years. Sectors such as payments solutions, wealth management, neo-banking, insurance technology solutions and data analytics are the other top sectors attracting foreign investment. In 2024, rural financing has also witnessed an uptick in investments.

Typically, up to 100% foreign direct investment under the automatic route is permitted for fintech companies that are regulated by the RBI or any other financial services regulator in India, subject to certain compliances such as minimum capitalisation norms. In the last 10 years, the Indian fintech industry has attracted USD 31 billion in investments, along with witnessing a start-up growth of 500 per cent. Of this, about USD 677 million has been raised in Q3 of 2024 (between July 1 and September 28, 2024) alone.

Overall, the Indian fintech sector is maturing. While the investments and deal activity in the Indian fintech space had been slowing after a peak in 2021, Q2&3 of 2024 saw a rebound in the investments and deal activity. As is typical, late-stage financing rounds (Series C+) attracted most investment. The share of angel and seed stage investments and deals also increased, while growth stage (Series A-B) fintech companies faced dampened interest.

Contributors

Shilpa Mankar Ahluwalia
Partner, Head- Fintech
shilpa.mankar@amsshardul.com

Himanshu Malhotra
Principal Associate
himanshu.malhotra@amsshardul.com

Purva Anand
Associate
purva.anand@amsshardul.com