International
Comparative
Legal Guides

Fintech

2024

Eighth Edition

Contributing Editors:
David Ives, David Shone & James Cook
Slaughter and May

glg Global Legal Group

Expert Analysis Chapter

Q&A Chapters

Q&A Chapters Continued

International
Comparative
Legal Guides

India

Manavi Jain

Anup Kumar

Arjun Khurana

G&W Legal

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and the state of the development of the market, including in response to the COVID-19 pandemic and ESG (Environmental, Social and Governance) objectives. Are there any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications)?

India has a range of active fintech businesses operating across areas such as lending (credit), payments (both peer-to-merchant (P2C) and peer-to-peer (P2P) transfers), investments and trading, personal finance and wealth, credit ratings, insurance, regulation, etc. With over 3,000 recognised fintech startups, India is among the fastest-growing fintech markets in the world and currently the third-largest fintech ecosystem globally, with the industry expected to be valued at around USD 150 billion by 2025; the industry's Total Addressable Market expected to be USD 1.3 trillion by 2025; Assets Under Management & Revenue to be USD 1 trillion by 2030; and Market Opportunity to be USD 2.1 trillion by 2030, respectively. In the financial year 2022–2023, India recorded over 130 million digital payments worth INR 139 lakh crore. In August 2023, the Unified Payments Interface (UPI) recorded the highest-ever volume of transactions at USD 10.58 billion – evidencing the pace at which the payments sector of the industry is growing. As a result of this current and estimated growth, it is believed that digital payments (non-cash) will constitute a majority of all payments by 2026 – although such reports and trends are often prone to hyperbole and best taken with several pinches of salt.

While domestic players (some of which have foreign investment) dominate the fintech industry in India as of now, the last few years have seen several foreign players enter the field as well – a trend that is expected to continue. With increasing internet penetration among the Indian public and some (questionable) policy changes having indirect consequences for the sector, fintech in India is looking at a period of compounding growth over the coming years – particularly (though not exclusively) in the payments sector, as also supported by the stats above. The domestic players and domestically developed tech are also breaking geographical barriers and aiming for global outreach – India's UPI is now accepted in seven countries: France; the UAE; Mauritius; Sri Lanka; Singapore; Bhutan; and Nepal.

The Indian fintech space continued to accelerate through the global COVID-19 pandemic, albeit with a few initial hiccups that affected business in general at the onset of the pandemic. The Reserve Bank of India (RBI) Deputy Governor, in a recent Bulletin, again recognised that the increase in financial inclusion the world over as well as the accelerated digitisation in India is attributable to the pandemic. The COVID-induced increased reliance on technology in general in the past few years, now removed, could potentially impact the industry in a negative manner in the coming years, at least for some sub-sectors. Other factors that could negatively impact the industry is the continued likelihood of a global recession and the ongoing geopolitical events across the world. A recent report by KPMG indicates a substantial decline in global fintech investments in 2023 – in India and other countries. However, some other reports continue touting fintech as an all-weather sector. As we estimated previously, the payments sub-sector appeared to have suffered comparatively less than the "traditional" sub-sectors; other sub-sectors like insurtech, ESG and cyber security also saw notable investments.

ESG objectives continue to become increasingly relevant for the financial space in general. Not only did the ESG sub-sector within the fintech space see notable investments, the year also saw a boom in fintechs making green financing more accessible, particularly for SMEs. In 2023, India witnessed its first recycled PVC card (rPVC) launched by Tide and Transcorp. Earlier, Indian regulators also tapped into this trend, with "Business Responsibility and Sustainability Reports" becoming mandatory for the top 1,000 listed companies in India, and a framework for regulating ESG Ratings Providers being further deliberated. The Innovation Hub (by the RBI) also has sustainable financial innovation as one of its objectives, and it recently released its guidelines on acceptance of green deposits. Further, International Financial Services Centres Authority (IFSCA)'s committee on sustainable finance submitted their report in October 2022 with recommendations towards realising their goal as a global sustainable hub – IFSCA also has a dedicated category of incentives/grants (Green FinTech Grant) focused on sustainable finance. Earlier, the Securities and Exchange Board of India (SEBI) had proposed guidelines to direct ESG fund managers to have at least 80% of their total assets in sustainability-themed securities from October 2022 onwards and has now also introduced an ESG category of mutual funds. Last year, India also incorporated sovereign green bonds. Per reports, climate and electric vehicle (EV) financing are likely to emerge as new areas of growth in the sector.

As expected, notable fintech trends that continue to see a definitive boom include Buy Now, Pay Later (BNPL) and other micro-credit options. In addition to the previously quoted trends of blockchain, open banking, increasing collaboration between fintech businesses and traditional banks, neo-banks, etc., embedded insurance and finance (which continues witnessing a drastic increase already, particularly in technology-related businesses), cyber security, fraud prevention, artificial intelligence (AI) and the metaverse were some notable trends of the year that went by. Digital payments continued to show an upward trend too – and the trend is likely to continue with India's international launch of the UPI.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Regulations applicable to fintech businesses in India are complex and evolving. Possible restrictions or prohibitions on a fintech company may depend on the regulations that apply to the business being undertaken by that entity. For example, a fintech business engaged in the acceptance of deposits and lending cannot undertake such business without the appropriate banking or non-banking licence from the RBI (India's central bank and regulator). For instance, despite the popularity of the BNPL fintech platforms in India, the RBI tightened its framework for these by issuing/amending its applicable circulars/guidelines – including issuing Guidelines on Digital Lending, RBI Master Directions on Credit Card and Debit Card – Issuance and Conduct, 2022 and a clarification to its earlier Master Directions on Prepaid Payment Instruments (MD-PPI).

In an attempt to concretise this further, the recently set up IFSCA in Gandhinagar, Gujrat (under the IFSCA Act, 2019) came up with a list of "illustrative" fintech and techfin areas/activities in India. The fintech activities are divided into three broad categories: the banking sector; capital markets and funds management; and the insurance sector, and expressly include BNPL, digital banks, robo advisory, sustainable finance products, embedded insurance, cyber insurance, etc. The techfin areas/activities expressly include agri tech, climate/green/sustainable tech, space tech, solutions for banking, financial services, defence tech, etc.

The true legal status of cryptocurrency continues to be a grey area in India. As of now, there is no specific regulation governing cryptocurrency-based businesses. Back in April 2018, the RBI had prohibited all banks and non-banking financial companies regulated by it from dealing in virtual currencies or providing any services for facilitating dealings in or settling of virtual currencies. This was challenged before the Supreme Court of India, which overturned the prohibition, stating that the RBI cannot impose any restrictions on the buying and selling of cryptocurrencies in the absence of a legislative bar.

The Government of India previously introduced the draft Cryptocurrency and Regulation of Official Digital Currency Bill, 2021 (Cryptocurrency Bill), which provided for: (a) the creation of a framework for official digital currency to be issued by the RBI; and (b) the prohibition of all private cryptocurrencies in India – with certain exceptions, to promote the underlying technology of cryptocurrency and its uses. The Bill has been stuck in limbo and the fate of it becoming a law is currently uncertain. In the 2022 Budget, the Government of India started taxing profits from the sale of virtual digital assets or "crypto" (with cryptoprofits being taxed at the same percentage rate as lottery winnings, which seems oddly telling in itself) and a proposed amendment seeks to make failure to pay taxes on the same a punishable offence. However, with India taking over the G20 presidency, it has been clarified that cryptocurrency is not illegal in India and that the International Monetary Fund is working with the G20 countries on a consultation paper for the regulation of cryptoassets. The RBI's release of a concept note on Central Bank Digital Currency (CBDC) in October 2022 as well as launching a pilot run for the same – both in wholesale and retail, supports the Government's idea of adopting a centralised digital currency (e-Rupee) – with more to be seen on how decentralised digital currencies are treated in the future. The RBI has also brought about relevant amendments to the RBI Act, 1934 to include currency in digital forms also.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Equity and debt funding are both available for growing businesses in India. For companies in general, (fintech or otherwise), the most common type of funding comes from private investors (venture capitalists or private equity funds). Business loans from banks and other financial institutions are also available, but loans are less popular owing to high interest rates and the need for proportionate collateral. Foreign investments, subject to the applicable laws, are also allowed in India. Indian companies have the option of raising funds by way of external commercial borrowings (ECB), which are foreign loans from recognised eligible lenders, such as foreign financial institutions, banks and foreign equity holders. IPOs are also common when it comes to the funding of fintechs.

The Government of India as well as the State Governments also bring out schemes and initiatives to bolster startups and growing businesses, from a funding perspective; some of which are listed below:

- Credit Guarantee Trust for Micro and Small Enterprise (which offers loans of up to INR 10 million without collateral to micro and small enterprises).
- Start-up India Initiative (which offers funding and incentives to eligible startups).
- PRISM's Technopreneur Promotion Program (which provides financial aid to individual innovators).
- Tamil Nadu FinTech Policy 2021 (offering collaboration and incentives for select fintech startups).

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Special incentives to promote investments are announced at the central and state levels – either through longer-term policy announcements, or periodic schemes. Many of these incentives are available only to domestic investors, but some are available to foreign investors as well.

Competitive tax rates levied on capital gains by investors is another way to attract investments. The Government also develops specific schemes, independently and under the National Manufacturing Policy (2011) and Make in India Programme (2014), aimed at creating infrastructure for increased investments in particular sectors. In the Budget for 2023–2024, the Government allocated INR 1,500 crore for fintech and banks. Last year, the Government had also announced an incentive of INR 2,600 crore for fintech startups and banks, for the promotion of UPI transactions. Similar incentives are likely in this year's Budget as well. Some other notable schemes/incentives include: Pradhan Mantri Jan Dhan Yojana (along with Aadhar – the unique biometric identification system and UPI – together referred to as the JAM Trinity), which aims at increasing financial inclusion in India and enabling fintech startups to build technology products to penetrate the large consumer base in India; and India Stack – a societal initiative aimed at building public digital infrastructure to promote public and private digital initiatives including accelerated adoption of technology in finance, etc.

The Government has also announced measures to specifically promote investments in tech/fintech/startup businesses in India, or that have had a positive impact on those sectors – for instance: the Startup India Investor Connect Portal; the Startup India Seed Fund Scheme; notification of faster exits for startups, etc. Additionally, IFSCA has also introduced an incentive scheme for, *inter alia*, domestic fintechs seeking access to overseas markets as well as foreign fintechs seeking market access to IFSCs in India. The Government also proposed many tax-related relaxations, including an extension of timelines (from March 31, 2023, to March 31, 2025) for funds relocation to GIFT City.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Conditions that need to be satisfied for a business to IPO are set out as "eligibility norms" by SEBI. These norms are laid down under various "routes". First, there is the **Profitability Route** – which mandates, *inter alia*, the minimum net tangible assets as well as the minimum net worth of a business to be eligible to IPO. Second, there is the **Alternative Route** – which mandates that a majority of the net offer to the public be allotted to Qualified Institutional Buyers (QIBs).

Additionally, there are conditions for anchor investors/directors/promoters of a business that are looking to IPO set out by SEBI, which include: a mandatory minimum contribution of promoters as well as a lock-in period on the shares owned by them; and a clean track record with SEBI and other law enforcement agencies in terms of disciplinary actions/offences. These compliance requirements were recently revised to be made more stringent, to reduce post-listing price volatility. There are "pricing guidelines" as well, again issued by SEBI, that come into play. Apart from these, certain National Stock Exchange (NSE) rules also need to be complied with.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Artivatic.ai, a fintech startup, was acquired by RenewBuy in a deal reportedly valued at USD 10 million. All its shareholders exited as a part of the transaction.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Owing to the overlapping and non-linear business models of fintech businesses, there is no single all-encompassing regulatory legal framework in India. The applicable laws and rules governing a fintech business will generally depend on the nature of the business being conducted.

Key regulators

Financial sector undertakings, including fintech businesses, are usually regulated by the RBI, SEBI, the Insurance Regulatory and Development Authority of India (IRDAI), the Pension Fund Regulatory and Development Authority (PFRDA), and IFSCA.

Aspects that are regulated by the aforementioned authorities include online payments and transactions, payment aggregators and gateways, data and privacy, lending and collection of deposits, trading of securities and derivatives, offering of insurance products and services, etc. For many financial offerings, prior approvals and licences need to be obtained from the RBI, SEBI or IRDAI for a business to commence.

The laws and regulations that may apply to fintechs in India are listed below:

RBI

- The RBI Act, 1934.
- The Banking Regulation Act, 1949.
- Payment and Settlement Systems Act, 2007.
- MD-PPIs, 2022.
- Framework for Scale Based Regulation for Non-Banking Financial Companies, 2021.
- Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries, 2009.
- Guidelines for Licensing of Payments Banks, 2014 and Operating Guidelines for Payments Banks, 2016.
- Framework for Recognition of a Self-Regulatory Organisation for Payment System Operators, 2020.
- Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2020.
- Circular on Processing of e-mandate on cards for recurring transactions, 2019.
- Circular on Tokenisation – Card transactions, 2019.
- Guidelines on Digital Lending, 2022.
- RBI Master Directions on Credit Card and Debit Card – Issuance and Conduct, 2022.

National Payments Corporation of India (NPCI)

- Various circulars on UPI payments.

SEBI

- Circular on Mutual Funds, 2021.
- Other relevant circulars, including those on Stock Exchanges and Clearing Corporations, Know Your Customer (KYC) Norms for the Securities Market, and Surveillance of the Securities Market.

IRDAI

- Guidelines on Insurance Repositories and Electronic issuance of Insurance Policies, 2015.
- Guidelines on Insurance e-commerce, 2017.
- IRDAI (Issuance of e-Insurance Policies) Regulations, 2016.

IFSCA

- IFSCA Act, 2019.
- Framework for FinTech Entity in the IFSCs, 2022.

MISC

- The Information Technology Act, 2000 and rules issued thereunder.
- The Indian Contract Act, 1872.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There is currently no dedicated regulation directed at cryptocurrencies or cryptoassets.

Please refer to our response to question 1.2 on regulations relating to cryptocurrencies or cryptoassets.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Financial regulators and policy-makers in India are becoming increasingly receptive to fintech innovation and technology-driven new entrants, as long as they fall within the purview of broadly established regulatory structures. However, things may not be as straightforward when dealing with disruptive innovation that does not fit neatly into existing regulatory frameworks – or innovations that further the likelihood of consumer deception or frauds. The RBI recently proposed setting up a FinTech Repository under the earlier announced Reserve Bank Innovation Hub (RBIH), recognising the use of emerging technologies like Distributed Ledger Technology (DLT), AI and machine learning, etc. by fintechs.

The primary market regulators have all come up with regulatory "sandbox" options for fintech businesses in India, with innovation being at the forefront of all of them:

RBI

In 2019, the RBI came up with an Enabling Framework for Regulatory Sandbox, under which the first cohort was announced later in the same year with the theme: "*Retail Payments*". In late 2021, it was reported that six entities had completed the test phase of the first cohort.

Subsequent themes for the second (announced in December 2020), third (announced in September 2021), and fourth cohorts (announced in October 2021) under the regulatory sandbox are "*cross border payments*", "*MSME Lending*" and "*Prevention and Mitigation of Financial Frauds*", respectively. The fifth cohort (announced in September 2022) was theme neutral – innovative products/services technologies cutting across various functions in the RBI's regulatory domain would be eligible to apply. In October 2023, eight entities commenced testing of their products under the third cohort towards MSME Lending, out of which, five were found viable resulting in their "exit".

Recently, the RBI also set up a separate "fintech department" to focus attention on the fintech sector.

SEBI

SEBI came up with the Framework for Regulatory Sandbox in 2020 (revised in 2021), aiming to promote innovation in the securities market and to grant facilities and flexibility to the entities regulated by SEBI to experiment with fintech solutions. SEBI has launched an online initiative called "Innovation Sandbox" to promote innovation in the fintech sector.

IRDAI

To promote innovation in the insurance space, IRDAI created a regulatory sandbox and notified the IRDAI (Regulatory Sandbox) Regulations in 2019. One of the main objectives of this sandbox is to strike a balance between orderly development of the insurance sector on the one hand and protection of the interests of policyholders on the other, while facilitating innovation. Recently, IRDAI also issued Guidelines on Operational Issues pertaining to the regulatory sandbox, which covers aspects of disclosure to the customers/participants by the participants of a sandbox, confidentiality of personal information and data security, etc.

IFSCA

IFSCA has set up numerous committees, including on sustainable finance. Through its framework, IFSCA also created a regulatory sandbox called the IFSCA Fintech Regulatory Sandbox (FRS). IFSCA also launched "I-Sprint" – a series of global cohorts and hackathons for fostering fintech innovation. IFSCA also has a "FinTech Hub" for attracting global talent.

Additionally, India also saw the setting up of mechanisms other than regulatory sandboxes to bolster innovation in the fintech industry. For instance: the Inter-Ministerial Steering Committee on FinTech (IMSC) was set up by the Department of Economic Affairs, which has met five times to discuss developments across the sector; the RBI set up the National Centre for Financial Education to promote awareness within the sector; and the Government set up Joint Working Groups with countries such as the UK and Singapore. In September 2022, as a part of an ongoing effort to promote collaboration, the Monetary Authority of Singapore (MAS) and IFSCA entered into a Fintech Cooperation Agreement. Among other things, the Agreement is likely to lead to further research and information sharing.

In 2022, an Inter-operatable Regulatory Sandbox was set up under the aegis of the sub-committee of the Financial Stability and Development Council (FSDC-SC) for inter-regulatory co-ordination among the financial sector regulators on fintech-related issues.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Until now, the biggest regulatory hurdle that a fintech business *established* outside India faced was the requirement for certain businesses to have a "local" presence in India. The scenario now, with the creation of IFSCA and implementation of the Framework for FinTech Entity in the IFSCs, could change this situation to an extent, with the framework being applicable to eligible foreign entities as well – in fact, reports suggest that Google is planning to open a dedicated FinTech Hub within GIFT City under IFSCA. In any case, foreign companies wishing to set up a business in India will have to comply with the applicable foreign exchange control regulations, including restrictions (if any) relating to the maximum permissible foreign ownership in an Indian entity/subsidiary.

Other concerns could emanate from issues such as cross-border transactions and payments – for instance, a fintech business engaged in lending/credit (which is facing tightening of regulations even for the domestic sector) may find itself facing regulatory restrictions around borrowing/lending in foreign exchange. Another example of a foreign fintech player doing business in India is PayPal, which had announced the winding up of its domestic payments business in India (already a highly competitive market) and instead focusing on international sales for Indian businesses. Recently, the RBI issued the Regulation on Payment Aggregators – Cross Border (PA-CB), bringing under its ambit payment aggregator entities facilitating cross-border payments.

Cyber security and data storage could be another hurdle to navigate, particularly with the coming into effect of India's first ever dedicated data protection legislation last year, and also under existing sectoral laws. For instance, the RBI mandates that all data related to payment systems be stored within India, which applies to businesses that are part of the payments ecosystem. This significantly impacts multinationals that transfer global payments data to centralised locations for storage and processing by default, or to locations outside India, at any rate. Indeed, there are a few marquee names in the financial services sector whose Indian business operations have been halted for non-compliance with data storage regulations.

Applicable equally to domestic as well as foreign players is the increased scrutiny of the regulators when it comes to the fintech sector. Recently, PayTM, a popular domestic fintech player, incurred strict operational sanctions by the RBI on account of its non-compliances and supervisory concerns.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The Information Technology Act, 2000 (IT Act) is the primary legislation in India governing matters of cyber security and data protection, and additionally provides legal validity to electronic documents and records. It prescribes specific cyber security offences and their associated penal action (including imprisonment provisions for certain offences), as well as compensation to affected parties in some instances.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) govern the currently applicable personal data protection regime in India. The SPDI Rules are slated to be replaced by a comprehensive data protection legislation, the Digital Personal Data Protection Act, 2023 (DPDP Act). The DPDP Act has been passed by the Indian legislature and will come into force upon a notification by the Indian Government to that effect, which is expected to happen sometime in 2024 although no official indications as to timelines has been provided by officials. As things stand, the collection, use, transmission, storage and processing of sensitive personal data of natural persons is governed by the SPDI Rules formulated under the IT Act.

The SPDI Rules prescribe certain restrictions with respect to the collection, storage, transfer, processing and disclosure of Sensitive Personal Data and Information (SPDI) – which has been defined to include: passwords; financial information such as bank account, credit card, debit card or other payment instrument details; physical, physiological and mental health data; sexual orientation data; medical records and history; and biometric information, etc. The SPDI Rules mandate that any corporate body collecting SPDI from any person must obtain the prior written consent of the data subject. Consent should be obtained in relation to the fact of collection of SPDI, the purpose of such collection, the proposed recipients of the data, etc. Also, consent must be obtained prior to the transfer or disclosure of SPDI, unless such transfer is part of a lawful contract between the parties. Further, the SPDI Rules require all corporate bodies that collect, store, use or transfer SPDI to maintain reasonable security practices and procedures, in line with International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements", or other standards duly approved and notified by the Central Government.

Under the SPDI Rules, every company that collects SPDI must appoint a Grievance Officer to address/redress grievances of data subjects. A company handling SPDI must also post its privacy policy on its website, which should comply with the SPDI Rules and should list, among other things, the kinds of SPDI being collected and the purpose and manner in which SPDI will be used.

Financial information, which is usually collected by fintech businesses, would fall under the definition of SPDI, and would thus be subject to the SPDI Rules.

The DPDP Act (slated to replace the SPDI Rules) places the same standards and requirements on all categories of personal data as opposed to the SPDI Rules. Personal data may be processed only under a lawful basis as provided in the DPDP Act, and consent remains the primary lawful basis for processing data. Consent under the DPDP Act must meet specified conditions – it must be provided through a positive action by the data subject and must be free, specific, informed, unconditional and unambiguous. Data subjects (referred to as "data principals" in the legislation) are also provided with enhanced rights, including the right to request for a summary of their personal data being processed and entities with whom the personal data has been shared, the right to access, review and correct their personal data, the right to withdraw consent and request for deletion of their personal data, and the right to a grievance redressal mechanism.

In addition to the SPDI Rules, several privacy focused regulations have been framed by regulators in India to ensure protection of financial information. For instance, IRDAI has framed several regulations, which require: (i) insurers to maintain confidentiality of insurance policyholders; (ii) that insurance records be held in data centres located in India; and (iii) that all data provided by insurance service providers to their outsourced service providers be retrieved immediately after provision of the services. There are specific regulations for insurance intermediaries and third-party administrators (commonly known as TPAs), including insurance brokers, insurance web aggregators, common service centres and insurance surveyors, regarding confidentiality and protection of insurance-related data received by them for servicing of insurance policies.

As mentioned previously, the RBI has also mandated that all Payment System Operators in the payment ecosystem ensure that the entire data relating to payment systems operated by them are stored on systems and data centres only in India. There is no prohibition on overseas *processing* of payments-related data, but data processed outside India should be deleted from the overseas systems and brought back to India no later than one business day or 24 hours from payment processing. Additionally, the data should include full end-to-end transaction details – details of information collected, carried and processed as part of the payment instruction. For the foreign leg of the transaction, if any, a copy of the data can also be stored in the foreign country, if required.

Furthermore, as per the Guidelines on Regulation of Payment Aggregators and Payment Gateways of the RBI, authorised non-bank payment aggregators and merchants on-boarded by them are prohibited from storing actual card data – except the last four digits of card numbers, which can be stored for reconciliation purposes.

Under the RBI Guidelines on Digital Lending, regulated entities need to ensure that any collection of data by digital lending apps/platforms is need-based only, with prior and explicit consent of the borrower and an audit trail. Further, the regulated entities also need to ensure that the digital lending apps/platforms desist from accessing mobile phone resources of the borrower – a one-time access can be taken for camera, microphone, location or any other necessary facility during on-boarding/KYC only, with the explicit consent of the borrower. Further, the Guidelines mandate regulated entities to ensure that the digital lending apps/platforms engaged by them do not store personal information of borrowers except basic minimal data; and that no biometric data is collected or stored unless allowed under the extant statutory guidelines.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The applicability of the SPDI Rules on foreign establishments is somewhat of a grey area, even though the IT Act (under which the SPDI Rules are framed) does contain provisions that extend its application beyond India in certain cases. As things stand, foreign organisations may still have to indirectly comply with certain aspects of Indian privacy laws by virtue of being service providers to Indian fintechs. For example, as per the SPDI Rules, an Indian entity cannot transfer SPDI to a foreign entity that does not adhere to the same level of data protection and security standards as that of the Indian entity (the transferor).

The SPDI Rules do not impose a blanket prohibition on the transfer of data outside India. Instead, cross-border transfers are allowed subject to certain conditions, namely: (a) that the transferee foreign entity ensures the same level of data protection that is adhered to by the transferor entity in India; **and** (b) express consent of the data subject has been obtained, unless the data transfer is part of a lawful contract between the data subject and the transferor.

Under the DPDP Act, there is no restriction on transferring personal data outside of India for the purposes of processing, as long as other umbrella requirements under the DPDP Act (such as lawful basis and consent) are fulfilled. However, the DPDP Act does grant the Central Government the power to notify countries to which such transfer is prohibited.

There are other sectoral regulations, however, that do restrict the cross-border transfer of data, or specify data storage, in certain cases. For instance, as mentioned earlier, IRDAI requires that insurance records are held in data centres located in India. Similarly, the RBI requires that all Payment System Operators in the payment ecosystem ensure that the entire data relating to payment systems operated by them are stored on systems and data centres in India. Under the RBI Guidelines on Digital Lending, explicit consent of the borrower needs to be taken before sharing personal information with any third party. Further, the Guidelines mandate that all data is stored only in servers located within India.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

If entities that are in possession of, handle or deal in SPDI are found to be negligent in their implementation and maintenance of reasonable security practices and procedures resulting in wrongful loss or gain to any person, they are liable to pay compensatory damages. The IT Act also penalises disclosure of information that is in breach of a lawful contract.

As for the DPDP Act, it makes a distinction between data controllers (referred to as "data fiduciaries") and data processors, and all compliance obligations fall squarely on data fiduciaries. Data fiduciaries are required to ensure that the above rights are provided to data principals and comply with the other requirements (such as a data breach notification requirement in addition to the one put in place by the Indian Computer Emergency Response Team (CERT-In)). Contraventions of the DPDP Act will be looked into by the Data Protection Board of India (a regulatory body set up through the DPDP Act) and are punishable with fines of up to INR 2.5 billion (approximately USD 30 million).

Under the Information Technology (CERT-In and Manner of Performing Functions and Duties) Rules, 2013 (the CERT-In Rules) framed under the IT Act, service providers, intermediaries, data centres and other entities are required to report cyber incidents to CERT-In (i.e., the authority that deals with cyber incidents) within a reasonable timeframe so that CERT-In can take timely action. Any failure to comply with this will attract a penalty of up to INR 5,000 for every day such failure continues. Furthermore, CERT-In has the power to call for information and give directions for the purpose of carrying out its functions. Any person who fails to provide the information called for, or comply with the direction of CERT-In, may be punished with imprisonment for a period up to one year or a fine of up to INR 10 million, or both.

Sanctions under specific laws (implemented and enforced by sectoral regulators such as the RBI, SEBI or IRDAI) are mostly in the form of fines/penalties but may also include imprisonment. The RBI and IRDAI also have clarificatory provisions for sanctions for offences committed by companies, which bring into their purview every individual who (at the time of any contravention by a company) was in charge of/responsible to the company for the conduct of business of the company – if the person had knowledge of the contravention and they did not exercise due diligence to prevent that contravention. In certain cases, the RBI and IRDAI may also order partial or full suspension of business activities due to violation of data localisation requirements, or data security lapses, or non-compliance with the prescribed security standards.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The IT Act and rules formed thereunder (such as, amongst others: the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018; the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021; the Information Technology (Electronic Service Delivery) Rules, 2011; and CERT-In Rules, which also provide for the creation of CERT-In, an administrative body responsible for collecting and analysing information on cyber security incidents) may have some bearing on issues pertaining to cyber security in the fintech space. Once notified, the DPDP Act may also have some bearing on some aspects of cyber security.

Beyond the IT Act, the RBI has also issued a comprehensive framework on cyber security that is currently applicable only to banks and non-banking financial institutions. Other circulars implemented by the RBI, for instance its MD-PPIs, have directions for PPIs to "establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches", and for non-bank PPIs to submit a System Audit Report (SAR), including a cyber security audit conducted by a CERT-In empanelled auditor, within two months of the close of its financial year. In June 2023, the RBI published draft Master Directions on Cyber Resilience and Digital Payment Security Controls for Payment System Operators (Draft Cybersecurity Directions) for public consultation and feedback.

SEBI has issued circulars on "Cyber Security Resilience framework for Stockbrokers/Depository Participants" and "Cyber Security Resilience framework for Mutual Funds/Asset Management Companies (AMCs)", which may also have some impact on fintech businesses.

IRDAI has issued Information and Cyber Security Guidelines containing a comprehensive cyber security framework for the insurance sector for implementing appropriate mechanisms to mitigate cyber risks.

Additionally, the Credit Information Companies (Regulation) Act 2005, the Credit Information Companies Regulations 2006, and Aadhaar (Targeted Delivery of Financial and Other Subsidiaries, Benefits, and Services) Act 2016 contain regulations on issues related to cyber security.

IFSCA also issued the IFSCA (Maintenance of Insurance Records and Submission of Requisite Information for Investigation and Inspection) Regulations, 2022, which impose a requirement for maintenance of records for, *inter alia*, cyber security policy and data protection.

The proposed Digital India Act would also possibly include a broader, overarching framework for cyber security, including setting up of a specialised and dedicated adjudicatory mechanism for resolution of cyber disputes.

Recently, the Central Consumer Protection Authority also issued Guidelines for Prevention and Regulation of Dark Patterns, 2023, which might have some bearing on incidents of cyber security.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The Prevention of Money Laundering Act, 2002 (PMLA) (along with the rules framed thereunder) is the primary anti-money laundering legislation in India. India is also a member of the Financial Action Task Force (FATF) and a signatory to various conventions that deal with anti-money laundering and countering financing of terrorism. Pursuant to the PMLA, and India's obligations as a member of the FATF and as a signatory to anti-money laundering conventions, an obligation has been cast on banking companies, financial institutions and intermediaries to maintain a record of financial transactions of a prescribed nature and value, furnish information relating to those transactions for verification, and maintain identity records of all its clients in the prescribed manner. Accordingly, financial regulators such as the RBI, SEBI and IRDAI have specific regulations and guidelines regarding maintenance of records of financial transactions and verification of customers; for example: (i) SEBI's Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT)/Obligations of Securities Market Intermediaries; (ii) RBI's Master Direction – KYC Direction, 2016 (which includes an obligation on certain players to report suspicious activity to a specific department of the Indian Central Government – FIU-IND); and (iii) IRDA's guidelines on Anti Money Laundering/Counter-Financing of Terrorism (AML/CFT) for the insurance sector.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction (for example, AI)?

Apart from what has already been mentioned, there are no other regulatory regimes that may apply to fintech businesses operating in India. Specifically with respect to AI, SEBI issued a circular requiring registered mutual funds offerings using AI and machine learning technologies to submit quarterly submissions to SEBI furnishing specifics like the technology used, safeguards in place to prevent abnormal behaviour of the AI, etc.

In the Budget for the year 2023–2024, it was announced that for realising the vision of Make AI in India and Make AI Work for India, three centres of excellence for AI will be set up in top educational institutions. AI – it has been predicted – will be a major theme in the Budget for the year 2024–2025 as well. The proposed Digital India Act will likely include provisions governing the implementation and use of AI technologies in India.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

India does not recognise the concept of at-will employment. As per the Industrial Disputes Act, 1948 (ID Act) and shops and establishment legislation of certain states, termination of employment should be undertaken for a reasonable cause.

Employees in India are broadly categorised into two groups: workmen; and non-workmen. The ID Act deals with industrial disputes and provides statutory protection to workmen in certain matters, such as termination, transfers and closure of establishments.

The ID Act defines a "workman" as any person who is employed in any industry to do any manual, unskilled, skilled, technical, operational, clerical or supervisory work for hire or reward, regardless of whether the terms of employment are express or implied. The following categories of employees are excluded from the definition of workmen:

- persons employed in an administrative or managerial capacity; and
- persons employed for supervisory work and earning more than INR 10,000 per month.

The definition of a workman is broad enough to cover most employees, except those performing managerial or supervisory functions. It is common for an employee to be performing (a) managerial or supervisory work, as well as (b) work that may be technical, skilled, unskilled or operational in nature. Several courts have ruled that where an employee performs multiple roles, the dominant nature of work performed by such a person in the usual course of business should be considered when deciding whether the employee is a workman or a non-workman. All employees other than workmen, namely employees performing managerial and supervisory functions, will fall under the category of non-workmen.

As per the ID Act, employment of a workman, who has been in continuous employment for not less than one year, may be terminated without any cause only after issuing a notice of one month (or payment of wages instead of the notice) and payment of compensation equivalent to 15 days' average pay for every completed year of continuous service. In certain cases, such as a manufacturing facility employing more than 100 workmen, the length of the termination notice is three months.

Unlike in the case of workmen, employment of a non-workman should be terminated in accordance with the employment agreement as well as the prevailing shops and establishment legislation of the jurisdiction where the relevant employee is employed. In many states, the applicable shops and establishment legislation requires that reasonable cause be established for termination of the services of an employee who has worked for a certain prescribed tenure.

The restrictions prescribed under the ID Act, employment contracts and the applicable shops and establishment legislation are always taken into consideration when dealing with cases of termination of employment.

5.2 What, if any, mandatory employment benefits must be provided to staff?

In India, employees are entitled to a host of mandatory benefits, some of which depend on factors such as tenure of employment and employee headcount. Some of the key benefits are mentioned below.

As per the Minimum Wages Act, 1948, salaries to employees should not be less than the minimum wages fixed by the respective State Government for a job. The shops and establishment legislation provides for: (i) paid (or earned), sick, casual and certain special leaves to employees; (ii) payment of overtime wages; and (iii) a safe and secure work environment. The Maternity Benefit Act, 1961, which is applicable to establishments employing at least 10 employees, provides for paid maternity leave and other benefits to female employees who have worked for at least 80 days in the 12 months immediately preceding their delivery date.

The Payment of Gratuity Act, which is applicable to establishments in which 10 or more employees are employed, mandates payment of gratuity benefits to employees who have been in continuous service for more than five years. Gratuity benefits are to be computed at the rate of 15 days' wages (at the rate of the last paid wages) for every year of continuous service, subject to a maximum prescribed cap.

The Employees' Provident Fund and Miscellaneous Provisions Act, 1952 (EPF Act) is a social security legislation that requires all establishments in India employing a minimum of 20 employees to make contributions towards provident fund schemes, pension schemes and deposit-linked insurance schemes in respect of all eligible employees (i.e., employees who earn less than INR 15,000 per month). Establishments employing fewer than 20 persons may voluntarily register under the EPF Act. Employers may even extend the benefits of the EPF Act to excluded employees (employees earning more than INR 15,000 per month).

The Employees' State Insurance Act, 1948 (ESI Act) is a social security legislation that (a) applies to employers having 10 or more employees overall, and (b) covers employees earning up to INR 21,000 per month (Covered Employees). The ESI Act mandates employers as well as Covered Employees to make contributions towards insurance and other schemes. Every month, employers are required to deposit with the Employees' State Insurance Corporation their prescribed employer contributions in respect of every Covered Employee.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

There are detailed requirements that need to be met for obtaining a work visa in India. Among others, these include the following: (i) the applicant should be a highly skilled or qualified professional; (ii) an employment visa will not be granted for jobs for which qualified Indians are available, or for routine, ordinary or clerical jobs; and (iii) the applicant being sponsored for an employment visa in any sector should draw a salary in excess of USD 25,000 *per annum*, except in certain limited, permitted cases.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

While there are multiple pieces of IP legislation in India, the ones that protect innovations and inventions are, amongst others: the Patents Act, 1970; the Copyrights Act, 1957; the Semiconductor Integrated Circuits Layout-Design Act, 2000; and the Designs Act. In terms of "technology", computer programs are *per se* not patentable in India unless they are tied to some hardware; software is typically protected through copyright law (through their underlying code). Products based on emerging technology, such as blockchain, non-fungible tokens and the metaverse, may find their home either in the Patents Act, 1970 or the Copyrights Act, 1957 – with the brands they are marketed under being protected through the Trademarks Act, 1999. The protection of innovations and inventions pertaining to AI is still being debated and discussed in India. In recommendations by a Standing Committee in Parliament (which was recently quoted by the Delhi High Court as well), it was recommended that the patents regime in India needs a review and revisions to be able to handle questions of AI innovations and inventions.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Please refer to our response to question 6.1 above for the various pieces of legislation under which IP may be protected in India.

While ownership may be recorded with the Indian IP office under any of the aforementioned pieces of legislation, actual ownership itself is a matter of fact and often flows from a contract. For instance, the inventor of a patentable innovation may assign their rights to an "applicant" for patent registration, or license them to a manufacturer for mass production. In case of software, a company may commission a third-party developer to code a software product, and choose to retain all or part of the copyright in that code, depending on the nature of the parties. In the absence of an agreement to the contrary, however, that copyright will, by default, rest with the party commissioning the work – such as in the case of a company whose employees create IP as part of their employment, in return for a salary or other remuneration. Most IP rights are assignable – with exceptions such as moral rights – with transfer of ownership flowing from contractual terms as well.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

While statutory rights in India undoubtedly provide the strongest protection and enforcement potential in most disputes, the absence of specific statutory rights may not preclude the option of enforcement entirely. In the case of trademarks, for instance, common law rights are also available in India – which accrue by local *use* of the mark, or by spill-over reputation. In case of copyrights as well, registration with the relevant authority is not mandatory and unregistered rights may be enforced as well. India is also a signatory to the Berne Convention for the Protection of Literary and Artistic Works and the Universal Copyright Convention, through which copyrights from signatory countries may be given protection in India, as well as the Agreement on Trade-Related Aspects of Intellectual Property Rights.

In terms of seeking statutory protection, the Madrid Protocol (for trademarks) and the Patent Cooperation Treaty (for patents) provide simplified application procedures through which parties can seek protection for their IP in multiple jurisdictions simultaneously, including in India.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP can be monetised by way of a straightforward sale of IP (which may entail a valuation exercise to arrive at a fair sale value), or by way of licensing or franchising to third parties in return for royalties or licence fees. Other options like securitisation and sale-leaseback arrangements may also be available.

Manavi Jain is a Managing Associate at G&W Legal and is a part of the Technology, IP and Media practice. She has advised several recognisable brands across various industries, including digital & media, hospitality, pharmaceuticals, sports, fashion & luxury goods, etc. on a broad spectrum of IP issues, with particular expertise in brand enforcement and brand management. Notably, she has advised a global hospitality company on complex licensing issues in Asia; assisted an Indian statutory body in enforcing its rights against an infringer at EUIPO; assisted a Europe-based sports governing body in enforcing its rights against infringers in India; and led settlement/co-existence negotiations in India for a global pharmaceuticals company.

Manavi also advises clients on issues pertaining to data protection and data privacy and assists digital businesses with setting up and scaling operations in India.

G&W Legal
C-9 / 9624, Vasant Kunj
New Delhi – 110070
India

Tel: +91 84473 79474
Email: manavi.jain@gnwlegal.com
LinkedIn: www.linkedin.com/in/manavi-jain-2631b851

Anup Kumar is a Partner at G&W Legal. He is part of the firm's General Corporate practice and leads on Regulatory Affairs. Over the years, Anup has developed an expertise in helping multinationals undertake business in India.

Anup advises clients globally in connection with India's myriad regulations, specialising in issues concerning: foreign investment; exchange controls; technology; and general corporate and regulatory compliance matters. He has developed an expertise in assisting clients navigate regulatorily complex sectors such as finance, F&B, Special Economic Zones, procurement and technology. Notably, Anup advises a large Australian retail chain in connection with their entry into and expansion in India; assists a UK company outsourcing their entire back-office operations to India on a variety of regulatory compliances; and advises a multinational consulting company on all regulatory aspects of its digital ventures in India.

G&W Legal
C-9 / 9624, Vasant Kunj
New Delhi – 110070
India

Tel: +91 72042 70364
Email: akumar@gnwlegal.com
URL: www.gnwlegal.com

Arjun Khurana is a Partner at G&W Legal. He chairs the firm's Technology, IP and Media practice and co-heads the Digital Business industry group.

Arjun's practice traverses: Privacy and Data Protection; Technology and Emerging Issues; Advertising and Marketing; IP; and Digital Ventures. He currently sits on INTA's Data Protection Committee and is a member of the International Association of Privacy Professionals. Arjun advises Fortune 500 companies as well as SMEs at the intersection of emerging tech and the law; guides clients through the changing data protection and privacy regime in India and allied regulatory frameworks; acts on complex cross-border technology transactions; and represents clients in commercial disputes. He has significant experience helping international businesses navigate the Indian legal landscape. Notably, Arjun represents one of the world's largest media networks in high-value litigation; advises an internet giant in connection with its AdTech business in India; counsels a global tech and consulting powerhouse on all aspects of its digital ventures vertical in India; advised a tech pioneer in connection with surveillance implications; and helps multiple multinationals steer through Indian digital payment regulations.

G&W Legal
C-9 / 9624, Vasant Kunj
New Delhi – 110070
India

Tel: +91 88001 16514
Email: arjun@gnwlegal.com
LinkedIn: www.linkedin.com/in/arjun-khurana-gnw

Combining the experience of Big Law with the expertise of a boutique, G&W Legal is a full-service business law firm that assists its clients at the intersection of law and pragmatism. Our team spans diverse subject matters and industries, using its robust skillset to become greater than the sum of its parts. In a short span, the firm and its attorneys have amassed a stellar reputation and received recognition from leading platforms such as *Chambers and Partners*, *Who's Who Legal*, *The Legal 500*, *WTR 1000* and the like.

As the world grows smaller in the information age, business is no longer limited by borders. We understand this well and provide our clients with advice and representation on every aspect of expanding into and doing business in India. Our attorneys bring a rich body of knowledge and accomplishment across (often intersecting) areas such as: Corporate/Commercial; Intellectual Property, Tech and Media; Franchising and Distribution; Advertising and Marketing; Privacy and Data Protection; Product Liability and Consumer Protection; International Trade; Foreign Investment; Private Equity and Venture Capital; Employment; Government Contracts; Corporate Restructuring; Corporate Governance, Ethics, Compliance and Investigations; Anti-trust/Competition; Regulatory Affairs; Real Estate; Dispute Resolution; and everything in between.

www.gnwlegal.com

G&W

Legal

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Fintech 2024 features one expert analysis chapter and 43 Q&A jurisdiction chapters covering key issues, including:

- The Fintech Landscape
- Funding For Fintech
- Fintech Regulation
- Other Regulatory Regimes / Non-Financial Regulation
- Accessing Talent
- Technology

The International Comparative Legal Guides are published by: glg Global Legal Group