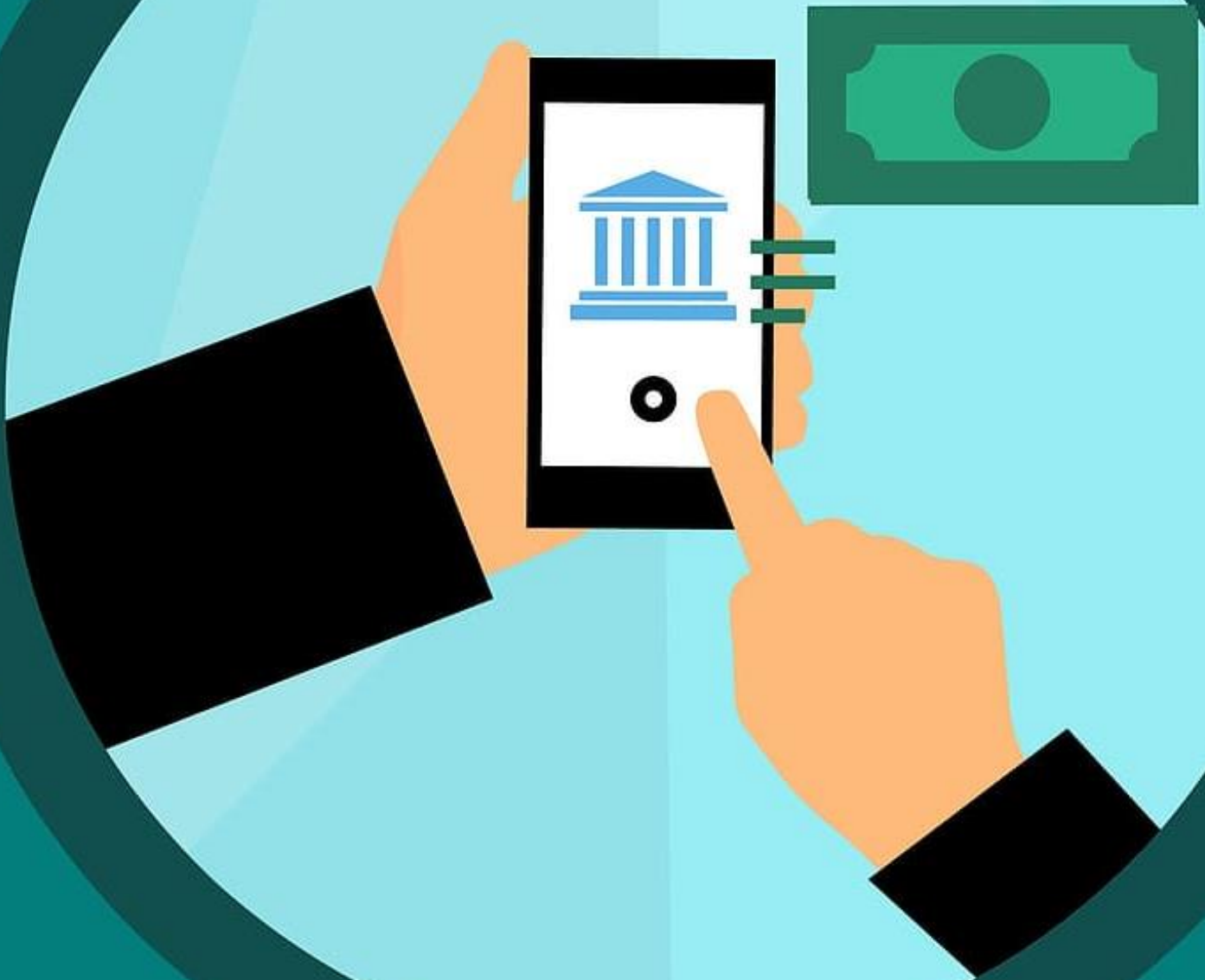


March 31, 2023



FINTECH PRIMER - II

argus
partners
SOLICITORS AND ADVOCATES

MUMBAI | DELHI | BENGALURU | KOLKATA

Introduction - Technology in Financial Transactions

Banks and other financial institutions have always been at the forefront of technology usage for their business purposes. This is usually driven by the need to cut costs, make more profits for shareholders and provide better customer service. The first Automatic Teller Machine (“ATM”) was set up in Mumbai in 1987. By 1997, there were around 1,500 ATMs in India. Soon telephone banking, which allows customers to perform over the telephone, a range of financial transactions which do not involve cash or financial instruments (such as cheques), without the need to visit a bank branch or ATM, became popular. As internet usage spread, internet banking became commonplace. As simple mobile phones were replaced by smart phones, mobile banking¹ gained momentum. FinTech businesses came in the wake of mobile banking.

FinTech

The term “FinTech” is short for “financial technology” and could apply to any kind of technology that is used to drive a financial transaction or service, offered by any entity. However, in business and regulatory jargon, FinTech has come to mean the technology used by financial service providers that disrupt the traditional way of providing such services. Thus, businesses such as PayTM, PhonePe, RazorPay, MobiKwik, PayU are all classified as fintech businesses.

Over the last 9 (nine) years, the Indian FinTech market has grown tremendously and consumer adoption of FinTech solutions has been increasing. Since Indian consumers have had positive experiences with tech firms offering non-financial services such as cab aggregation and hotel bookings, they came to expect and demanded similar standards from FinTech service providers. India was one of the largest and fastest growing FinTech markets, according to a 2022 report by EY². In fact, digital transactions in India in 2022 was more than four times that in USA, Britain, Germany and France combined, according to Indian Electronics & Information Technology Minister, Ashwini Vishnaw.³ India has a fintech adoption rate of 87% against the global average of 64%.⁴

Payment and Settlement Systems Act, 2007

The Payment and Settlement Systems Act, 2007 (“**P&SS Act**”) was enacted in December 2007 in order to provide for the regulation and supervision of payment systems in India. The P&SS Act designates the Reserve Bank of India (“**RBI**”) as the authority for such purpose. A “payment system” is defined to mean a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange. As per section 4 of the P&SS Act, an authorisation issued by the RBI is required, in order to commence or operate a payment system. Systems enabling the operation of credit or debits cards, smart cards, prepaid payment instruments would qualify as payment systems.

Regulation of Prepaid Payment Instruments by the RBI

Prepaid Payment Instruments (“**PPIs**”) are instruments which facilitate the purchase of goods and services, including financial services, remittance facilities, etc., against the value stored on such instruments. On October 11, 2017, the RBI issued the Master Direction on Issuance and Operation of Prepaid Payment Instruments (“**2017 PPI Master Directions**”) under section 18 read with section 10(2) of the P&SS Act. The 2017 PPI Master Direction consolidated the various circulars

¹ Mobile banking needs to be distinguished from telephone banking and internet banking. In mobile banking, customers download an application developed by the relevant bank to conduct financial transactions remotely, through a smartphone.

² https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/topics/consulting/2022/ey-winds-of-change-india-fintech-report-2022.pdf

³ <https://www.nytimes.com/2023/03/01/business/india-digital-payments-upi.html>

⁴ <https://www.drishtiiias.com/>

that had been issued by the RBI, until then, regarding the issuance and operation of PPIs. Further, in light of the various amendments made to the 2017 PPI Master Directions since 2017, the RBI issued the Master Directions on Prepaid Payment Instruments (PPIs) (“**PPI Master Directions/PPI MD**”) on August 27, 2021⁵. The salient features of the PPI Master Directions are as follows.

The PPI Master Directions state that no entity can set up and operate payment systems for PPIs without the prior approval/ authorisation of RBI.

Meaning and categorisation of PPIs

As per Para 2.8 of the PPI Master Directions, “Prepaid Payment Instruments” are instruments that facilitate purchase of goods and services, financial services, remittance facilities, etc., against the value stored therein. PPIs that require RBI approval / authorisation prior to issuance are classified under two types: (i) Small PPIs, and (ii) Full-KYC PPIs. Detailed features of such PPIs have been mentioned below.

It is interesting to note that while the 2017 PPI Master Directions categorised PPIs that could be issued in India into three categories: (i) Closed System PPIs, (ii) Semi-closed System PPIs and (iii) Open System PPIs, the PPI MD does not specifically make the above-mentioned categorisation. The PPI MD simply defines ‘Closed System PPIs’ as follows: “PPIs issued by an entity for facilitating the purchase of goods and services from that entity only and does not permit cash withdrawal. These instruments cannot be used for payment or settlement for third party services. The issuance or operation of such instruments is not classified as a payment system requiring approval / authorisation by RBI and are, therefore, not regulated or supervised by RBI.” Hence, any ‘Closed System PPIs’ are outside the purview of the PPI MD.

The PPIs that require RBI’s authorisation for issuance have not been categorised into open or semi closed PPIs. Instead, such PPIs have been classified into (i) small PPIs and (ii) full-KYC PPIs, depending upon whether full KYC is required to be done before such PPI can be issued.

Salient features of Small PPIs and Full-KYC PPIs

Paragraph 9.1 of the PPI Master Directions prescribes further limits on cash loading for PPIs, along with various operational requirements, including the Know Your Customer (“**KYC**”) documents to be obtained, which are as follows:

- (a) **Small PPIs:** PPIs of up to Rs. 10,000 (Rupees ten thousand) may be issued with minimum details of the PPI holder. The minimum details shall necessarily include mobile number verified with One Time Password (“**OTP**”) and self-declaration of name and unique identification number of any of the ‘officially valid documents’ defined under rule 2(d) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (“**PMLR**”). The amount loaded during any month or the outstanding amount in the PPI at any point of time shall not exceed Rs. 10,000 (Rupees ten thousand). Further, the total amount loaded during the financial year shall not exceed Rs. 1,20,000 (Rupees one lac twenty thousand). Such PPIs may be used only for purchase of goods and services. Cash withdrawal from such PPIs or fund transfers from such PPIs to bank accounts or to PPIs of the same or other issuers is not permitted.

Note that the Small PPIs have been further categorised into two types: (i) PPIs with cash loading facility and (ii) PPIs with no cash loading facility. Both the types of Small PPIs shall be reloadable in nature, however, the reloading in the latter may only be done through a bank account / credit card / full-KYC PPI. Further, the former type of Small PPI has an additional restriction – the total amount to be debited from such PPI during any month shall not exceed Rs.10,000. Moreover, Small PPIs with cash loading facility shall be converted into full-KYC PPIs (as defined in paragraph 9.2 of the PPI MD) within a period of 24 months from the date

⁵ Last updated as of February 10, 2023.

of issue of the PPI, failing which no further credit shall be allowed in such PPIs. There is no such requirement for a Small PPI with no cash loading facility.

- (b) **Full KYC PPIs:** PPIs of up to Rs 1,00,000 (Rupees one lac) may be issued after completing full KYC of the PPI holder. The Video-based Customer Identification Process, as detailed in the RBI Master Direction on KYC dated February 25, 2016, can be used to open full-KYC PPIs as well as to convert Small PPIs into full-KYC PPIs. The amount outstanding at any point of time in such PPIs shall not exceed Rs. 2,00,000 (Rupees two lac). These PPIs shall be used for purchase of goods and services, funds transfer or cash withdrawal.

The fund transfer limit shall be Rs 10,000 (Rupees ten thousand) per month, except in the case of “pre-registered beneficiaries”, being beneficiaries registered by the PPI holder. Such pre-registered beneficiaries shall have a fund transfer limit of Rs. 2,00,000 (Rupees two lac) per month. The funds can be transferred ‘back to source account’ (payment source from where the PPI was loaded) or ‘own bank account of the PPI holder’ (duly verified by the PPI issuer). Further, funds transfer from such PPIs shall also be permitted to other PPIs, debit cards and credit cards as per the limits given above.

Further, in case of bank issued PPIs, cash withdrawal shall be permitted. However, cash withdrawal at PoS devices shall be subjected to a limit of Rs.2,000 (Rupees two thousand) per transaction within an overall monthly limit of Rs.10,000 (Rupees ten thousand) across all locations, subject to conditions stipulated in RBI circular on “Cash Withdrawal at Point-of-Sale (POS) - Enhanced limit at Tier III to VI Centres” dated August 27, 2015.

In case of non-bank issued PPIs, cash withdrawal shall be permitted up to a maximum limit of Rs.2,000 (Rupees two thousand) per transaction within an overall monthly limit of Rs.10,000 (Rupees ten thousand) per PPI across all channels (agents, ATMs, PoS devices, etc.).

Eligibility criteria for non-banks

The PPI Master Directions prescribe the eligibility criteria for banks and non-banks to issue PPIs. For non-banks, the criteria are as follows:

- a) should be a company incorporated in India and registered under the Companies Act, 1956 / Companies Act, 2013.
- b) if regulated by any of the financial sector regulators, should submit a ‘No Objection Certificate’ from its regulator, to the RBI, when seeking authorisation under the PSS Act.
- c) shall have a minimum positive net worth of Rs. 5,00,00,000 (Rupees five crore) as per its latest audited balance sheet at the time of submitting the application, which shall be certified by its chartered accountant(s). By the end of the third financial year from the date of receiving final authorisation, the entity is required to have a minimum positive net worth of Rs. 15,00,00,000 (Rupees fifteen crore). The net worth has to be maintained by the entity at all times.
- d) shall be required to submit a net-worth certificate every year, to evidence compliance with the applicable net-worth requirement, within six months of completion of that financial year.
- e) If the non-bank entity has any foreign direct investment (“FDI”) or foreign portfolio investment (“FPI”) or foreign institutional investment (“FII”), such non-bank entity is additionally required to meet the capital requirements under the consolidated FDI policy guidelines of Government of India, as applicable and as amended from time to time.

As per the RBI Circular on “Perpetual Validity for Certificate of Authorisation (CoA) issued to Payment System Operators (PSOs) under Payment and Settlement Systems Act, 2007” dated December 4, 2020, the RBI shall issue a certificate of authorization authorising the issuance of PPIs on a perpetual basis, subject to the following conditions :

- a) full compliance with the terms and conditions subject to which authorisation was granted;
- b) fulfilment of entry norms such as capital, networth requirements, etc.;

- c) no major regulatory or supervisory concerns related to operations of the PSO, as observed during onsite and / or offsite monitoring;
- d) efficacy of customer grievance redressal mechanism; and
- e) no adverse reports from other departments of RBI / regulators / statutory bodies, etc.

Guidelines regarding issuance, loading and validity of PPIs

Paragraph 7 of the PP MD lays down certain guidelines regarding issuance, loading and reloading of PPIs. Cash loading to PPIs shall not exceed Rs. 50,000 (Rupees fifty thousand) per month, subject to the overall limit of the PPI. Further, PPIs may be issued as cards, wallets, and in any such form / instrument which can be used to access the PPI and to use the amount therein. No PPI shall be issued in the form of paper vouchers.

Para 13 of the PPI MD lays down the guidelines regarding validity and redemption of the PPIs. The important guidelines are as follows:

- a) All PPIs shall have a minimum validity period of one year from the date of last loading / reloading in the PPI. PPIs can be issued with a longer validity as well.
- b) The PPI Issuer shall clearly indicate the expiry period of the PPI to the customer at the time of issuance of PPIs. Such information shall be clearly enunciated in the terms and conditions of sale of PPI.
- c) PPI issuer shall caution the PPI holder at reasonable intervals, during the 45 days' period prior to expiry of the validity period of the PPI.
- d) In case the PPI holder approaches the PPI issuer for refund of the outstanding balance in the PPI, at any time within a period of three years from the expiry date of PPI, then the same shall be paid to the PPI holder in a bank account.

PPIs for Cross-border outward transactions

Para 8 of the PPI MD specifies that Banks having an AD-I licence are permitted under the PPI Master Directions to issue to Indian residents in India, reloadable semi closed or open system Full-KYC INR denominated PPIs, to be used in cross-border outward transactions. However, such use is limited to permissible current account transactions under the Foreign Exchange Management Act, 1999 ("**FEMA**"). Such PPIs cannot be used for any cross-border outward fund transfer and/or for making remittances under the RBI's Liberalised Remittance Scheme. Prefunding of a merchant's online account shall not be permitted using such Rupee denominated PPIs.

A PPI issuer may enable the facility of cross-border outward transactions only on explicit request of the PPI holders and shall apply a per transaction limit not exceeding Rs. 10,000 (Rupees ten thousand) and a per month limit not exceeding Rs. 50,000 (Rupees fifty thousand) for such cross-border transactions. In case such PPIs are issued in card form, then the PPI has to be Europay, Mastercard, Visa (EMV) Chip and PIN compliant.

PPIs for credit towards cross-border inward remittance

Banks and Non-bank PPI issuers, who have been appointed as the Indian agent of an authorised overseas principal, can issue INR denominated Full-KYC PPIs to beneficiaries of inward remittance under the Money Transfer Service Scheme ("**MTSS**") of the RBI. Such PPIs shall be issued in compliance with the MTSS Guidelines issued by the RBI. Amounts only up to Rs. 50,000 (Rupees fifty thousand) from individual inward MTSS remittances are permitted to be loaded or reloaded in full-KYC PPIs issued to beneficiaries. Amounts in excess of Rs. 50,000 (Rupees fifty thousand) shall be paid by credit to a bank account of the beneficiary.

Foreign Exchange PPIs:

The PPI MD provides that entities authorised under FEMA to issue foreign exchange denominated PPIs shall be outside the purview of the PPI MD. This implies that the issuance and operation of foreign exchange denominated PPIs shall continue to be governed by relevant regulations issued under FEMA.

Specific Categories of PPIs that may be issued by banks and non-banks

Para 10 of the PPI MD lays down that banks and non-banks shall not issue PPIs of any category other than the following categories:

- a) **Gift PPIs:** Maximum value of each such prepaid gift instrument shall not exceed Rs.10,000 (Rupees ten thousand). Such instrument shall not be reloadable. Cash-out or funds transfer shall not be permitted for such instrument.
- b) **PPIs for Mass Transit Systems (PPI-MTS):** These PPIs shall be issued by MTS operators after authorisation to issue such PPIs under the PSS Act. Such PPIs shall contain the Automated Fare Collection application related to transit service to qualify as such. Apart from MTS, such PPIs shall be used only at those merchant outlets whose activities are allied / related to or are carried on within premises of the MTS. PPI issuer may decide about customer details, if any, required to be obtained for issuance of such PPIs. PPI-MTS issued shall be reloadable in nature and maximum value outstanding in such PPIs shall not exceed the limit of Rs.3,000 (Rupees three thousand) at any point of time. Cash-out or refund or funds transfer shall not be permitted.
- c) **PPIs to Foreign Nationals / Non-Resident Indians (NRIs) visiting India:** Banks / Non-banks permitted to issue PPIs can issue INR denominated full-KYC PPIs to foreign nationals / NRIs visiting India, after physical verification of Passport and Visa of the customers at the point of issuance. The PPIs can be issued in the form of wallets linked to UPI and can be used for merchant payments (P2M) only. Loading / Reloading of such PPIs shall be against receipt of foreign exchange by cash or through any payment instrument. The conversion to Indian Rupee shall be carried out only by entities authorised to deal in Foreign Exchange under FEMA. The amount outstanding at any point of time in such PPIs shall not exceed the limit applicable on full-KYC PPIs.

Regulation of Payment Intermediaries by the RBI

Payment intermediaries include all entities which collect monies received from customers for payment to merchants using any electronic/online payment mode, for goods and services availed by them and thereafter facilitate the transfer of these monies to the merchants in final settlement of the obligations of the paying customers. However, intermediaries who facilitate transactions which are akin to a delivery versus payment arrangement shall not fall under the definition of a payment intermediary.

Until March 2021, there were two major RBI guidelines governing the sphere of payment intermediaries, namely:

- a. Directions For Opening And Operation Of Accounts And Settlement Of Payments For Electronic Payment Transactions Involving Intermediaries dated November 24, 2009 ("**2009 EPT Directions**"); and
- b. Guidelines on Regulation of Payment Aggregators and Payment Gateways dated March 17, 2020 ("**PAPG Guidelines**").

The **2009 EPT Directions** were issued by the RBI under section 18 of the P&SS Act with a view to safeguard the interests of the customers and to ensure that the payments made by them are

duly accounted for by the intermediaries receiving such payments and remitted to the accounts of the merchants who have supplied the goods and services without undue delay.

Similarly, the **PAPG Guidelines** were also issued under section 18 read with section 10(2) of the P&SS Act. The PAPG Guidelines came into effect from April 1, 2020 other than for activities for which specific timelines were mentioned. Further, through a notification dated March 31, 2021 ("**PAPG Notification 2021**"), the RBI made public certain clarifications on the PAPG Guidelines, issued by it on September 17, 2020. Through the PAPG Notification 2021, RBI repealed the 2009 EPT Directions with effect from June 30, 2021, except for Payment Aggregators ("**PAs**") whose application for authorisation was pending with the RBI.

Payment Aggregators ("**PAs**") are entities that facilitate e-commerce sites and merchants to accept various payment instruments from the customers for completion of their payment obligations without the need for merchants to create a separate payment integration system of their own. PAs enable merchants to connect with acquirers. In the process, PAs receive payments from customers, pool and transfer them on to the merchants after a time period. RBI clarified in the PAPG Notification 2021 that e-commerce marketplaces availing the services of a PA shall also be considered as merchants. Payment Gateways ("**PGs**") are entities that provide technology infrastructure to route and facilitate processing of an online payment transaction without any involvement in the handling of such funds.

The 2009 EPT Directions applied to "intermediaries", which is wider than, but includes PAs and PGs. With the advent of the PAPG Guidelines, which state that they will '*regulate in entirety the activities of PAs*', it was speculated that the 2009 EPT Directions will cease to apply to PAs who will now be bound solely by the PAPG Guidelines. RBI cleared the air by stating in the PAPG Notification 2021 that the 2009 EPT Directions shall be considered repealed for authorised PAs from the date of authorisation. The PAPG Guidelines also '*provide baseline technology-related recommendations to PGs*', which PAs are required to mandatorily adopt.

The PAPG Guidelines have detailed rules regarding: (i) the criteria for receiving authorisation as a PA or a PG; (ii) capital requirements; (iii) governance; (iv) merchant on-boarding; (v) settlement and escrow account management by non-bank PAs of the amount collected by them; and (vi) security, fraud prevention and risk management framework. While the PAPG Guidelines are to be mandatorily adhered to by PAs, PGs may or may not adhere to the baseline technology-related recommendations provided in the guidelines.

A PA shall be a company incorporated in India under the Companies Act, 1956 or the Companies Act, 2013 and the memorandum of association of the PA applying for registration must cover the proposed activity of operating as a PA. While banks carrying on the activity of a PA do not need any separate authorisation, non-bank entities which offer PA services will have to apply for authorisation on or before June 30, 2021. The PAPG Guidelines prohibit e-commerce marketplaces which also provide PA services to continue providing such activities beyond June 30, 2021 and mandate such marketplaces to separate their PA activities from the marketplace business, if they desire to continue conducting PA activities.

The PAPG Notification 2021 categorically states that the PA Guidelines are not applicable to 'delivery versus payment' transactions, such as hotel bookings and travel tickets, however, they cover transactions where the payment is made in advance while the goods are delivered in a deferred manner.

To meet the eligibility requirement, existing PAs as on the date of the PAPG Guidelines need to achieve a net-worth of Rs. 15,00,00,000 (Rupees fifteen crore) by March 31, 2021 and a net-worth of Rs. 25,00,00,000 (Rupees twenty five crore) by the third financial year, i.e., on or before March 31, 2023 which shall be maintained at all times thereafter. New PAs need to have a minimum net-worth of Rs. 15,00,00,000 (Rupees fifteen crore) at the time of application for authorisation and

shall attain a net-worth of Rs. 25,00,00,000 (Rupees twenty five crore) by the end of the third financial year of grant of authorisation which must also be maintained at all times thereafter.

The PAPG Guidelines state that the PAs shall be professionally managed, and the promoters of the entity have to satisfy the 'fit and proper criteria' prescribed by RBI. . The PAPG Notification 2021 laid down the 'fit and proper criteria'. Director of the PA company shall be deemed to be a "fit and proper" person if:

- a) Such person has a record of fairness and integrity, including but not limited to:
 - i. financial integrity;
 - ii. good reputation and character; and
 - iii. honesty.

- b) Such person has not incurred any of the following disqualifications:
 - i. Convicted by a court for any offence involving moral turpitude or any economic offence or any offence under the laws administered by the RBI;
 - ii. Declared insolvent and not discharged;
 - iii. An order, restraining, prohibiting or debaring the person from accessing / dealing in any financial system, passed by any regulatory authority, and the period specified in the order has not elapsed;
 - iv. Found to be of unsound mind by a court of competent jurisdiction and the finding is in force; and
 - v. Is financially not sound.

RBI has reserved with itself the final say in case any question arises as to whether a person is a fit and proper. PAs shall have a board approved policy for merchant on-boarding and shall undertake background and antecedent checks before on boarding merchants. However, the PAPG Notification 2021 clarified that the PA would not be required to carry-out the KYC process in accordance with the KYC guidelines of Department of Regulation, in cases where the merchant already has a bank account which is being used for transaction settlement purpose. PAs will be responsible for making sure that the merchant's infrastructure is compliant with data security standards as prescribed and does not store any customer card and related data.

Non-bank PAs shall maintain the amount collected by them in an escrow account with any scheduled commercial bank. An additional escrow account may be maintained with a different scheduled commercial bank at the discretion of the PA. Just like the 2009 EPT Directions, the PAPG Guidelines also list out the permissible credits and debits to the escrow account and the timelines for settlement with the merchant, however the timelines and classifications of the settlements are different. Amounts deducted from the customer's account shall be remitted to the escrow account maintaining bank on a Tp+0 / Tp+1 basis, where 'Tp' stands for the date of charge / debit to the customer's account against the purchase of goods / services. For the final settlement with the merchant by the PA, where the PA is responsible for delivery of goods or services, the payment to the merchant shall be not later than on Ts + 1 basis, where 'Ts' is the date of intimation by the merchant to the intermediary about shipment of goods. Where the merchant is responsible for delivery, the payment to the merchant shall be not later than on Td + 1 basis, where 'Td' is the date of confirmation by the merchant to the intermediary about delivery of goods to the customer. Where the agreement with the merchant provides for keeping the amount by the PA till expiry of refund period, the payment to the merchant shall be not later than on Tr + 1 basis, where 'Tr' is the date of expiry of refund period as fixed by the merchant. However, it appears that these timelines are not mandatory since the PAPG Notification 2021 states that there can be different "t" for different merchants as per the agreement between PA and merchants. Where PAs have no control over incoming funds and its delay thereof, the PAs need to follow the instructions and transfer the funds to the merchant within T+0 / T+1 basis, post receiving of funds into its account. PAs are permitted under the PAPG Guidelines to pre-fund the escrow account with their own or

the merchant's funds. However, in the latter scenario, the merchant's beneficial interest shall be created on the pre-funded portion.

The PAPG Guidelines provide for certain 'Baseline Technology-related Recommendations' on aspects such as security and information technology systems, information security governance, data security standards, security incident reporting, information technology governance, risk assessments etc. Apart from the security related recommendations, certain other recommendations include restrictions on storage of customer card credentials, instructions on storage of payment system data, refunds to be made and authentication of cards. As mentioned earlier, these recommendations are to be mandatorily adopted by PAs but are non-binding on PGs.

Payment Banks

A payments bank functions like a bank but operates on a smaller scale and cannot advance loans or issue credit cards. Such banks are registered as public limited companies under the Companies Act, 2013, and licensed under section 22 of the Banking Regulation Act, 1949, with specific licensing conditions restricting its activities mainly to the acceptance of demand deposits and provision of payments and remittance services.

The Guidelines for Licensing of Payment Banks dated November 27, 2014 was issued by the RBI with the objective of furthering financial inclusion by providing: (i) small savings accounts; and (ii) payments/remittance services to migrant labour workforce, low income households, small businesses, other unorganised sector entities and other users.

The Operating Guidelines for Payments Banks dated October 6, 2016 were issued as a need was felt for separate operating guidelines for payments banks, considering the differentiated nature of business and financial inclusion focus of these banks.

The minimum paid-up equity capital for payments banks is Rs.100,00,00,000 (Rupees one hundred crore). Each payment bank is required to have a leverage ratio of not less than 3% (three percent), that is, its outside liabilities should not exceed 33.33 times its net worth (paid-up capital and reserves). The promoter's minimum initial contribution to the paid-up equity capital of such payments bank shall at least be 40% (forty percent) for the first 5 (five) years from the commencement of its business. Foreign shareholding in payment banks is permitted in accordance with the FDI policy for private sector banks. Currently, 74% (seventy four percent) FDI is permitted in private sector banking (which includes payments banks), of which, up to 49% (forty nine percent) is permitted through the automatic route and beyond 49% (forty nine percent) and up to 74% (seventy four percent) is permitted through the government approval route.

As mentioned above, payment banks are not allowed to undertake lending activities. Moreover, such banks are required to invest a minimum of 75% (seventy five percent) of their "demand deposit balances" in Statutory Liquidity Ratio eligible Government securities/treasury bills with maturity up to 1 (one) year. Payment banks must also hold a maximum of 25% (twenty five percent) of their "demand deposit balances" in current and time/fixed deposits with other scheduled commercial banks for operational purposes and liquidity management, apart from amounts maintained as Cash Reserve Ratio with the RBI on its outside demand and time liabilities.

Payments banks were initially prohibited from holding more than Rs. 1,00,000 (Rupees one lac) per individual customer at the end of each day. However, on April 8, 2021, considering the progress made by payment banks in financial inclusion, the RBI enhanced the permitted maximum balance from Rs. 1,00,000 (Rupees one lac) to Rs. 2,00,000 (Rupees two lacs) per individual customer of payment banks with immediate effect.

InsurTech

When technology is used to provide a disruptive insurance related service, it is called InsurTech. Some of the leading InsurTech players in India are Acko, Policy Bazaar and Digit Insurance. The Insurance Regulatory and Development Authority of India (“**IRDA**”), the insurance regulator in India, issues guidelines and policies to regulate InsurTech in India.

Guidelines on Insurance e-commerce dated March 9, 2017 (“**Insurance e-Commerce Guidelines**”) have been issued by the IRDA. Insurance e-Commerce Guidelines enable insurers and insurance intermediaries to set-up Insurance Self-Network Platforms (“**ISNPs**”) to sell and service insurance policies. ISNP has been defined under these guidelines to mean an electronic platform set-up by any applicant with the permission of the IRDA. The Insurance e-Commerce Guidelines lay down the manner and procedures of grant of permission for establishing an ISNP for undertaking insurance e-commerce activities in India as well as the code of conduct to be adhered to by ISNPs.

The IRDA enacted the Insurance Regulatory and Development Authority of India (Insurance Web Aggregators) Regulations, 2017, with the objective to supervise and monitor web aggregators as an insurance intermediary who maintains a website for providing an interface to the insurance prospects for price comparison and information of products of different insurers and other related matters. Such insurance web aggregators have to obtain a certificate of registration from the IRDA to carry out their activities. Their activities include, *inter alia*, displaying product comparisons on insurance web aggregator website, selling insurance online or through tele marketing and other such marketing activities.

The IRDA has issued Guidelines on Standard Professional Indemnity Policy for Insurance Brokers, Corporate Agents, Web Aggregators, and IMF which came into effect from July 1, 2022. Under these guidelines, every general insurer should endeavour to offer the standard professional indemnity insurance for insurance brokers, corporate agents, web aggregators and insurance marketing firms. The policy must cover all damages arising from claim for breach of duty of the insured, fraud and dishonesty of any employee which the insured becomes legally liable to pay arising out of claims first made in writing against the insured during the policy period including legal costs and expenses incurred with prior consent of the insurers. A break in policy continuity or non-purchase of professional indemnity policy by intermediaries will result in penal action as per the guidelines.

UPI and BHIM

Unified Payments Interface (“**UPI**”) is a system that powers multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, seamless fund routing & merchant payments into one hood. It also caters to the “Peer to Peer” collect request which can be scheduled and paid as per requirement and convenience.

Bharat Interface for Money (“**BHIM**”) is a payment application that facilitates simple, easy and quick transactions using UPI. It is possible to make direct bank payments to anyone on UPI using the payee’s UPI ID or by scanning the payee’s quick response (“QR”) code with the BHIM application. A person may request money through the app from a UPI ID.

UPI and BHIM have been developed by the National Payments Corporation of India (“**NPCI**”), an umbrella organisation for operating retail payments and settlement systems in India. The NPCI is an initiative of the RBI and the Indian Banks’ Association under the provisions of the P&SS Act for creating a robust payment and settlement infrastructure in India.

Considering the utilitarian nature of the objects of NPCI, it has been incorporated as a “Not for Profit” Company under the provisions of section 25 of Companies Act, 1956 (now section 8 of Companies Act, 2013), with an intention to provide infrastructure support to the entire

banking system in India for physical as well as electronic payment and settlement systems. The 10 (ten) core promoter banks of NPCI are State Bank of India, Punjab National Bank, Canara Bank, Bank of Baroda, Union Bank of India Limited, Bank of India Limited, ICICI Bank Limited, HDFC Bank Limited, Citibank N. A. and Hongkong and Shanghai Banking Corporation. In 2016 the shareholding was broad-based to 56 (fifty six) member banks to include more banks representing all sectors.

Currently, only banks are allowed to integrate UPI into their online portals or mobile applications for use by their customers. However, banks may tie-up with non-banks for the provision of technology or design or operation of UPI powered payments.

The UPI Procedural Guidelines and the UPI Operating and Settlement Guidelines have been issued by NPCI in October, 2019 and these provide for various requirements that have to be complied with by an entity to participate in UPI as a payment systems provider. The guidelines prescribe, *inter alia*, the entities who can participate in UPI, such as payment service providers, their roles and responsibilities, permissible transactions that may be carried out by such payment services providers and their liabilities. The guidelines also prescribe rules for settlement of UPI transactions.

NPCI, through a circular NPCI/UPI/OC-97/2020-21 dated November 5, 2020, has issued guidelines for UPI third-party application providers such as Googlepay, PhonePe etc., to cap their respective market shares to thirty percent (30%). This is done to ensure that UPI volumes do not get concentrated in the hands of a few players. NPCI has stated in the aforementioned circular that the said 30% volume cap is to be calculated on the basis of the volume of transactions processed during the preceding three months (on a rolling basis). Vide a circular dated December 2, 2022, NPCI has extended the deadline for implementation of these guidelines from December 2022 to December 2024.

Through a circular dated July 5, 2022, NPCI has mandated that UPI applications may capture geographic locations and details of customers only with their consent. Further, such collection of location / geographical details cannot be mandatory and the option to enable / revoke consent should be provided to the customer.

Vide a circular dated January 10, 2023, NPCI has allowed NRIs from ten countries including Singapore, Australia, Canada, UK operating non-resident external ("**NRE**") and non-resident ordinary ("**NRO**") bank accounts to access UPI through their international mobile numbers. This facility for NRIs shall be subject to member banks ensuring that the accounts of the NRIs are in adherence with foreign exchange regulations and guidelines issued by the RBI from time to time.

Cryptocurrencies

A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology—a distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.⁶

The RBI has always taken a dim view of cryptocurrencies, termed "virtual currencies" in its circulars. Through public notices issued December 24, 2013, February 1, 2017 and December 5, 2017, the RBI cautioned users, holders and traders of virtual currencies, including Bitcoins, regarding various risks associated in dealing with such virtual currencies. Through a circular dated April 6, 2018, the RBI pronounced that, with immediate effect, entities regulated by the RBI shall not deal in cryptocurrencies or provide services for facilitating any person or entity in dealing with

⁶ <https://www.investopedia.com/terms/c/cryptocurrency.asp>.

or settling cryptocurrencies (“**RBI Circular**”). The prohibited services included maintaining accounts, registering, trading, settling, clearing, giving loans against virtual tokens, accepting them as collateral, opening accounts of exchanges dealing with them and transfer/ receipt of money in accounts relating to purchase/ sale of cryptocurrencies. Entities regulated by the RBI which were already providing such services were called on to exit the relationship within 3 (three) months from the date of the aforementioned RBI Circular.

The Internet and Mobile Association of India and various crypto exchanges and traders filed writ petitions challenging the RBI Circular on several grounds including, *inter alia*, that since the RBI Circular forbade banks from extending a range of services to facilitate entities dealing with cryptocurrencies, the virtual currency exchanges would shut down and that there was lack of proportionality in the RBI Circular in that the regulatory action was disproportionate to the goals that such action was seeking to achieve. On March 4, 2020, the Supreme Court of India in the case of *Internet and Mobile Association of India v. Reserve Bank of India*,⁷ struck down the RBI Circular and thereby the curb on cryptocurrency trade in India. The Supreme Court held as follows:

“The position as on date is that VCs are not banned, but the trading in VCs and the functioning of VC exchanges are sent to comatose by the impugned Circular by disconnecting their lifeline namely, the interface with the regular banking sector. What is worse is that this has been done (i) despite RBI not finding anything wrong about the way in which these exchanges function and (ii) despite the fact that VCs are not banned.

....

It is no doubt true that RBI has very wide powers not only in view of the statutory scheme of the 3 enactments indicated earlier, but also in view of the special place and role that it has in the economy of the country. These powers can be exercised both in the form of preventive as well as curative measures. But the availability of power is different from the manner and extent to which it can be exercised. While we have recognized elsewhere in this order, the power of RBI to take a pre-emptive action, we are testing in this part of the order the proportionality of such measure, for the determination of which RBI needs to show at least some semblance of any damage suffered by its regulated entities. But there is none. When the consistent stand of RBI is that they have not banned VCs and when the Government of India is unable to take a call despite several committees coming up with several proposals including two draft bills, both of which advocated exactly opposite positions, it is not possible for us to hold that the impugned measure is proportionate.” (emphasis supplied)

However, even whilst striking down the RBI Circular, the Supreme Court also held that anything that may pose a threat to, or have an impact on, the financial system of the country, can be regulated or prohibited by the RBI, despite the said activity not forming part of the credit system or payment system. Evidently, the RBI failed to convince the Supreme Court that cryptocurrencies pose a threat to or have an impact on the financial system of the country.

P2P lending platforms

P2P lending is a type of crowd-funding wherein people who want to borrow money can raise funds through loans from people who want to invest. It may be done through online platforms that match lenders with borrowers to provide unsecured loans. Such form of lending eliminates the need to have financial institutions as intermediaries and provides recourse to borrowers who are unable to obtain credit from financial institutions.

The Master Directions – NBFC – Peer to Peer Lending Platform Directions, 2017 (“**P2P Directions**”) were issued by the RBI under sections 45IA, 45JA, 45L, and 45M of the Reserve Bank of India Act, 1934 (“**RBI Act**”), to provide a framework for the registration and operation of non-banking financial companies (“**NBFC**”) in India which carry on the business of a peer to peer lending platform. A peer-to-peer lending platform is defined in the P2P Regulations as an

⁷ Writ Petition (Civil) No.528 of 2018 with Writ Petition (Civil) No.373 of 2018.

intermediary providing the services of loan facilitation via an online medium or otherwise, to persons who have entered into an arrangement with an NBFC-P2P to lend on it or to avail of loan facilitation services provided by it.

The P2P Directions cap the aggregate exposure of a lender to all borrowers across all P2P platforms, at Rs. 50,00,000 (Rupees fifty lac). Further, such investments by lenders through P2P platforms need to be consistent with their net-worth. Any lender investing more than Rs. 10,00,000 (Rupees ten lac) across the P2P platforms has to produce a certificate to such platforms from a chartered accountant certifying a minimum net-worth of Rs. 50,00,000 (Rupees fifty lac).

The aggregate loans taken by a borrower at any point of time, across all P2Ps, are subject to a cap of Rs. 10,00,000 (Rupees ten lac) and the exposure of a single lender to the same borrower, across all P2Ps, shall not exceed Rs. 50,000 (Rupees fifty thousand). The P2P Directions limit the maturity of the loans to 36 (thirty-six) months.

Ombudsman Scheme

The [Reserve Bank – Integrated Ombudsman Scheme, 2021](#) (“the Ombudsman Scheme”) came into effect from November 12, 2021 and amalgamated the (i) the Banking Ombudsman Scheme, 2006; (ii) the Ombudsman Scheme for Non-Banking Financial Companies, 2018; and (iii) the Ombudsman Scheme for Digital Transactions, 2019. The Ombudsman Scheme sets out the procedure for appointment of an ombudsman by the RBI, caps the tenure of an ombudsman or a deputy ombudsman to three years, details the powers, functions and the procedure, which the Ombudsman shall follow for redressal of complaints.

The Ombudsman Scheme defines “System Participant” under Clause 3(1)(l) to mean “a person other than the Reserve Bank and a System Provider, participating in a payment system as defined in the Payment and Settlement Systems Act, 2007” and a “System Provider” under Clause 3(1)(m) to mean and include “a person who operates an authorised payment system as defined in Section 2 of the Payment and Settlement Systems Act, 2007”. The Ombudsman Scheme has defined regulated entities under clause 3(1)(j) in a very wide manner to include banks, NBFCs, System Participants and any other entity as may be specified by the Reserve Bank from time to time. Therefore, all services provided by any regulated entity would fall under the regulatory purview of the Ombudsman Scheme, which is general in its application and applies to digital transactions as well.

Currently around 22 (twenty-two) ombudsmen for digital transactions have been appointed with their offices located mostly in state capitals. According to the [annual report of ombudsman schemes, 2021-22](#), dated January 4, 2022, Ombudsmen dealt with 3,04,496 (three lac four thousand four hundred ninety six) complaints out of 4,18,184 (four lac eighteen thousand one hundred eighty four) complaints till November 11, 2021. Further, of these complaints, complaints relating to digital modes of payments and transactions were the highest, [amounting to 42.12%](#) of all the complaints.

Applicability of NBFC Regulations

An entity, which carries on FinTech business, may have to be registered with the RBI as an NBFC if it falls within the prescribed criteria.

An NBFC has been defined in section 45I(f) of the RBI Act as follows:

““non-banking financial company” means–

- (i) a financial institution which is a company;

- (ii) *a non-banking institution which is a company and which has as its principal business the receiving of deposits, under any scheme or arrangement or in any other manner, or lending in any manner;*
- (iii) *such other non-banking institution or class of such institutions, as the Bank may, with the previous approval of the Central Government and by notification in the Official Gazette, specify;*

Vide press release 1998-99/1269 dated April 8, 1999, the RBI had announced that in order to identify a particular company as an NBFC, it will consider both, the assets and the income pattern as evidenced from the last audited balance sheet of the company to decide its principal business. The company will be treated as an NBFC if its financial assets are more than 50% (fifty percent) of its total assets (netted off by intangible assets) and income from financial assets is more than 50% (fifty percent) of the gross income. Both these tests are required to be satisfied as the determinant factor for principal business of a company. This is also referred to as the “asset income” test.

The “asset income” test has been reiterated by the RBI in a notification issued by the RBI dated October 19, 2006 titled “*Amendment to NBFC regulations - Certificate of Registration (CoR) issued under Section 45-IA of the RBI Act, 1934 – Continuation of business of NBFI - Submission of Statutory Auditors Certificate – Clarification*”.

In terms of section 45-IA of the RBI Act, no NBFC can commence or carry-on business of a non-banking financial institution without: (a) obtaining a certificate of registration from the RBI and without having a net owned fund of Rs. 25,00,000 (Rupees twenty-five lac) and not exceeding Rs. 100,00,00,000 (Rupees one hundred crore). However, in terms of the powers given to the RBI, to obviate dual regulation, certain categories of NBFCs which are regulated by other regulators are exempted from the requirement of registration with RBI. Thus, an InsurTech business, which is regulated by the IRDA, does not have to be registered with the RBI. Vide its master circular bearing number RBI/2015-16/15 DNBR (PD) CC.No.052/03.10.119/2015-16 dated July 1, 2015, the RBI had provided that companies registered under Section 25 of the Companies Act, 1956 (now, Section 8 of the Companies Act, 2013) are exempt from registering as an NBFC with the RBI. Now vide Master Direction - Reserve Bank of India (Regulatory Framework for Microfinance Loans) Directions, 2022 issued by the RBI, on March 14, 2022, the RBI has reduced the exemption to Section 8 companies which provide microfinance loans⁸ and have an asset size of less than INR 100,00,00,000 (Indian Rupees one hundred crore) only.

Anti-Money Laundering Laws and KYC

In keeping with global moves to fight the laundering of proceeds of crime, drug sales and other forms of dirty money, India enacted the Prevention of Money Laundering Act, 2002 (“**PMLA**”) and the PMLR, which came into effect from July 1, 2005. The PMLA and PMLR impose obligations on banking companies, financial institutions and intermediaries to verify the identity of clients, maintain records and furnish information in a prescribed form to the Financial Intelligence Unit - India (“**FIU-IND**”). FIU-IND was set up by the Government of India vide an office memorandum dated November 18, 2004 as the central national agency responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and financing of terrorism. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (“**EIC**”) headed by the Indian Finance Minister.

⁸ As per the Reserve Bank of India (Regulatory Framework for Microfinance Loans) Directions, 2022, a microfinance loan is a loan given to a borrower whose monthly household income does not exceed INR 3,00,000 (Indian Rupees three lakh). Further the monthly loan obligations of the borrower’s household cannot exceed 50% of the monthly household income.

The Master Direction on KYC dated February 25, 2016 (“**KYC Master Directions**”), issued by the RBI, applies to all “Regulated Entities”, which is defined by regulation 3(b)(xiii) of the KYC Master Directions to include, *inter alia*, all Payment System Providers (“PSPs”) / System Participants (“SPs”) and Prepaid Payment Instrument Issuers (“PPI Issuers”). The KYC Master Directions require all Regulated Entities to implement a KYC policy, a customer acceptance policy and a risk based approach for risk management.

Regulated Entities are required to undertake identification of customers: (i) at the time of commencement of an account-based relationship with the customer; (ii) when carrying out any international money transfer operations for a person who is not an account holder of the bank; (iii) when there is a doubt about the authenticity or adequacy of the customer identification data it has obtained; (iv) selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than Rs. 50,000 (Rupees fifty thousand); (v) carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds Rs. 50,000 (Rupees fifty thousand), whether conducted as a single transaction or several transactions that appear to be connected; (vi) when a Regulated Entity has reason to believe that a customer (account-based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000 (Rupees fifty thousand). Vide an amendment dated April 1, 2021 to the Master Direction on KYC – KYC Norms For Self Help Groups (SHGs), sub-clause (c) of Section 43 was amended to provide that customer due diligence of all the members of a self-help group shall be undertaken when credit-linking is being done. Prior to this amendment, Section 43(c) had provided that no separate customer due diligence is required at the time of credit linking of SHGs.

Section 57 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (“Aadhaar Act 2016”) permitted private companies to use aadhaar to establish the identities of individuals. Further, the Aadhaar (Authentication) Regulations, 2016, (“Aadhaar Regulations”) permitted an entity that was authorised to use e-KYC authentication facilities under the Aadhaar Regulations to share the e-KYC data of the holder of the aadhaar number with other entities for a specified purpose, subject to the consent of the concerned individual having been obtained. Many Fin-Tech companies that had online operations were reliant on the OTP based e-KYC in order to comply with the requirement of the customer identification process, which was recognised under the Aadhaar Act 2016 and the KYC Master Directions.

On September 26, 2018 the Supreme Court of India in the case of *Justice Puttaswamy (Retd.) v. Union of India*,⁹ (“Aadhaar Case”) struck down parts of the Aadhaar Act that permitted the use of an individual’s aadhaar number to establish the identity of such individual for any purpose by private businesses. As a result of this judgement, companies are no longer able to use the authentication facilities authorized under the Aadhaar Regulations.

In the Aadhaar Case, while striking down a part of section 57 of the Aadhaar Act 2016 as violative of the fundamental right to privacy of individuals to the extent it allowed any company or any person to use the aadhaar numbers to establish the identity of individuals for *any purpose* pursuant to a contract, the Supreme Court observed as follows:

“Insofar as Section 57 in the present form is concerned, it is susceptible to misuse inasmuch as: (a) It can be used for establishing the identity of an individual ‘for any purpose’. We read down this provision to mean that such a purpose has to be backed by law. Further, whenever any such “law” is made, it would be subject to judicial scrutiny. (b) Such purpose is not limited pursuant to any law alone but can be done pursuant to ‘any contract to this effect’ as well. This is clearly impermissible as a contractual provision is not backed by a law and, therefore, first requirement of proportionality test is not met. (c) Apart from authorising the State, even ‘any body corporate or person’ is authorised to avail authentication services which can be on the basis of purported agreement between an individual and such body corporate or

⁹ Writ Petition (Civil) No. 494 OF 2012.

person. Even if we presume that legislature did not intend so, the impact of the aforesaid features would be to enable commercial exploitation of an individual biometric and demographic information by the private entities. Thus, this part of the provision which enables body corporate and individuals also to seek authentication, that too on the basis of a contract between the individual and such body corporate or person, would impinge upon the right to privacy of such individuals. This part of the section, thus, is declared unconstitutional. (emphasis supplied)

Post the Aadhaar Case, FinTech companies have been developing innovative methods for onboarding new customers without aadhaar based authentication. While some companies have started using video-based authentication that uses government issued identifications like PAN cards, drivers licenses and passports with further innovations underway, others have been using selfie-based identification through mobile phones. Through these new methods of customer authentication, the costly route of physical verification has been avoided.¹⁰ For instance, a peer to peer lending platform developed a video-based customer authentication application through which the 'liveliness test' of a customer could be obtained. At the end of the loan approval process, the camera in the applicant's phone or laptop prompts the customer to read the displayed writing. If the customer is able to read the writing, the application matches the video with the applicant's photograph and draws a conclusion about the identity of the person. Similarly, some companies in the digital lending space have developed a video-based solution that uses PAN cards to verify the genuineness of customers. An applicant is prompted to move their head right or left, hold their PAN card and read out their PAN card number while the application in the phone or laptop records the process.¹¹

The Unique Identification Authority of India ("UIDAI") a statutory authority established under the Aadhaar Act 2016 has introduced an offline QR code for aadhaar that holds users' non-sensitive details and the user is not required to share their aadhaar number, biometrics or mobile number with private entities.

SEBI, vide its circular titled SEBI/HO/MIRSD/DOP/CIR/P/2020/73, dated April 24, 2020, titled "Clarification on Know Your Client (KYC) Process and Use of Technology for KYC", has provided that an investor's KYC may be completed via online / App based KYC, in-person verification through video, online submission of Officially Valid Document (OVD) / other documents under eSign. SEBI further declared that –

- i. e-sign service,
- ii. an electronic equivalent of a document, with a valid digital signature issued by the issuing authority of the document, including those documents that are issued to the digital locker account of the investor as per Rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016, and
- iii. electronic signatures, including eSign mechanism of aadhaar shall be accepted in lieu of wet signature and all these three would be accepted as technological innovations facilitating online KYC.

The aforementioned circular also prescribes features for online KYC apps of the SEBI registered intermediaries may have and use for undertaking online KYC of investors. It also provides deeper guidance into details that may help ease the process of getting a KYC done online, such as which documents would fall under the purview of officially valid documents in terms of Rule 2(d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and explains the process of how the apps may enable video in person verification of investors.

¹⁰https://www.business-standard.com/article/companies/post-sc-ruling-fintechs-replacing-aadhaar-with-innovative-e-kyc-processes-119052800238_1.html.

¹¹ *Ibid.*

Vide a circular SEBI/HO/MIRSD/DOP/CIR/P/2020/80 dated May 12, 2020, SEBI listed those entities that may undertake aadhaar authentication service of UIDAI as a KYC user agency (“**KUA**”) in securities market. The circular also mandates the KUA to allow SEBI registered intermediaries/ mutual fund distributors to undertake aadhaar authentication of their clients for the purpose of KYC. Vide the circular SEBI/HO/MIRSD/SEC-5/P/CIR/2022/99, dated July 20, 2022, SEBI mandated the 155 (one hundred and fifty five) reporting entities notified by the Department of Revenue – Ministry of Finance, Government of India to enter into an agreement with a KUA and register themselves with UIDAI as sub-KUAs.

Now, vide circular IRDAI/SDD/CIR/MISC/016/01/2021 dated January 22, 2021, the Insurance Regulatory and Development Authority of India (“**IRDAI**”) extended the Central KYC Registry to legal entities as well. Thus, reporting entities shall now be required to upload the KYC data pertaining to accounts of legal entities opened on or after April 1, 2021 on to CKYCR in terms of Rule 9(1A) of the PML Rules.

Regulatory Sandbox for FinTech

A sandbox is a safe environment where parents let their children play without the fear of them getting hurt. In order to encourage innovation in FinTech, the RBI has facilitated the establishment of a FinTech sandbox where banks and FinTech players can experiment with innovative financial products or services or newly developed technologies for a specific duration and within safe boundaries. Within a sandbox, the characteristics exhibited by the production environment are mimicked on a real-time basis, generating responses from all the systems that such a product or application would interface with. Appropriate safeguards would be in place to help contain the consequences of any failure.

RBI has issued an Enabling Framework for Regulatory Sandbox dated August 13, 2009 (“**RS Framework**”). As per the RS Framework, the entities eligible to participate are FinTech companies, including start-ups, banks, financial institutions and any other company partnering with or providing support to financial services businesses. The regulatory sandbox is meant to be a medium to encourage innovations intended for use in the Indian market in areas where: (i) there is an absence of governing regulations; (ii) there is a need to temporarily ease regulations for enabling the proposed innovation; and (iii) the proposed innovation shows promise of easing/effecting delivery of financial services in a significant way.

The RS Framework provides an indicative list of innovative products, services and technology which could be considered for testing under the regulatory sandbox:

Innovative Products/Services

- Retail payments
- Money transfer services
- Marketplace lending
- Digital KYC
- Financial advisory services
- Wealth management services
- Digital identification services
- Smart contracts
- Financial inclusion products
- Cyber security products

Innovative Technology

- Mobile technology applications (payments, digital identity, etc.)
- Data Analytics
- Application Program Interface (APIs) services
- Applications under block chain technologies
- Artificial Intelligence and Machine Learning applications

The RS Framework also provides an indicative negative list of products, services and technologies which may not be accepted for testing under the rules, such as:

- Credit registry
- Credit information
- Crypto currency/ Crypto assets services
- Trading/investing/settling in crypto assets
- Initial Coin Offerings, etc.
- Chain marketing services
- Any other product/service which has been banned by the regulators/Government of India.

RBI's Inter-Operable Regulatory Sandbox

Vide a press release 2022-2023/1030 dated October 12, 2022, the RBI came out with a standard operating procedure for inter-operable regulatory sandbox, which may be applicable for hybrid products or services falling under the purview of multiple regulatory authorities. According to the press release, financial regulators which are members of the Inter-Regulatory Technical Group on FinTech had consented to participate in the arrangement and the Fintech department of the RBI would act as the nodal point for receiving applications under the sandbox. The dominant features of the product, its eligibility criteria and network would be criterias to adjudge the participant's entry into the regulatory sandbox. While the concerned regulator shall reserve the right to admissibility of the hybrid product or innovation, detailed scrutiny of the application shall be done by the concerned regulatory based on its own framework. However, this step by RBI seems to mark a big step in the right direction allowing for FinTech innovations to be tested faster and more efficiently.

Sandbox For Capital Markets

SEBI, vide circular SEBI/HO/MRD-1/CIR/P/2020/95 dated June 5, 2020, allowed participants in the capital market to test out the solution in a controlled environment without deploying the innovation as a whole.

Sandbox For InsurTech

The IRDA notified the Insurance Regulatory and Development Authority of India (Regulatory Sandbox) Regulations, 2019 ("IRDAI RS") on July 26, 2019 with the objective of striking a balance between the orderly development of the insurance sector on one hand and the protection of interests of policyholders on the other, while at the same time facilitating innovation. The IRDAI RS was meant to be in force for a period of 2 (two) years from the date of its publication in the official gazette. The IRDAI RS has now been amended by the Insurance Regulatory and

Development Authority of India (Regulatory Sandbox) (Amendment) Regulations, 2022 and will now be in effect indefinitely.

This regulatory sandbox provides a controlled regulatory environment to insurance companies to carry out assessments of any of its innovative products and technologies. The IRDAI RS allows an applicant to seek permission from IRDAI for promoting or implementing innovation in insurance sector in the following:

- Insurance Solicitation or Distribution
- Insurance Products
- Underwriting
- Policy and Claims Servicing
- Any other category recognised by IRDA.

The IRDAI RS also prescribes the procedure for making such applications to the IRDA as well as the conditions for granting such permission to applicants. The maximum duration for the experimental period was six (6) months. However, pursuant to the IRDAI Sandbox Amendment, this time limit has been extended to thirty-six (36) months. Further, the maximum extension that may be granted post expiry of the above-mentioned time period has also been increased to twelve (12) months from six (6) months.

Tokenisation

Framework for device-based tokenisation

In 2019, the RBI issued a circular “Tokenisation - Card transactions”, dated January 8, 2019 (“**2019 Tokenisation Circular**”), wherein the RBI permitted authorised card payment networks to offer card tokenisation services to any token requestor (i.e., third party app provider), subject to certain specified conditions.

In terms of the 2019 Tokenisation Circular, “Tokenisation” refers to replacement of actual card details with a unique alternate code called the “token”, which shall be unique for a combination of card, token requestor and device (referred hereafter as “**identified device**”).

The 2019 Tokenisation Circular provides for the following conditions to be fulfilled for offering tokenisation services:

- a) Tokenisation and de-tokenisation shall be performed only by the authorised card network and recovery of original Primary Account Number (PAN) should be feasible for the authorised card network only. Adequate safeguards shall be put in place to ensure that PAN cannot be found out or obtained from the token and/or vice versa, by anyone except the card network. Integrity of token generation process shall be ensured at all times.
- b) Tokenisation and de-tokenisation requests should be logged by the card network and available for retrieval, if required.
- c) The actual card data, token and other relevant details of the card shall be stored in a secure mode. Token requestors shall not store the PAN or any other card related detail.
- d) The card network shall get the token requestor certified for (a) token requestor’s systems, including hardware deployed for this purpose, (b) security of token requestor’s application, (c) features for ensuring authorised access to token requestor’s app on the identified device, and, (d) other functions performed by the token requestor, including customer on-boarding, token provisioning and storage, data storage, transaction processing, etc.
- e) Card networks shall get the card issuers/acquirers, their service providers and any other entity involved in payment transaction chain, certified in respect of changes done for processing tokenised card transactions by such persons.
- f) All certification/security testing by the card network shall conform to international best practices/globally accepted standards.

- g) Registration of card on token requestor's app shall be done only with explicit customer consent through Additional Factor of Authentication (AFA), and not by way of a forced/default/automatic selection of check box, radio button, etc.
- h) AFA validation during card registration, as well as, for authenticating any transaction, shall be as per the existing RBI regulations for authentication of card transactions.
- i) Customers shall have option to register/de-register their card for a particular use case, i.e., contactless, QR code based, in-app payments, etc.
- j) Customers shall be given option to set and modify per transaction and daily transaction limits for tokenised card transactions.
- k) Suitable velocity checks (i.e., how many such transactions will be allowed in a day/week/month) may be put in place by card issuers/card network as considered appropriate, for tokenised card transactions.
- l) For performing any transaction, the customer shall be free to use any of the cards registered with the token requestor app.
- m) Secure storage of tokens and associated keys by token requestor on successful registration of card shall be ensured.
- n) Card issuers shall ensure easy access to customers for reporting loss of "identified device" or any other such event which may expose tokens to unauthorised usage. Card network, along with card issuers and token requestors, shall put in place a system to immediately de-activate such tokens and associated keys.
- o) Dispute resolution process shall be put in place by card network for tokenised card transactions.
- p) Card network shall put in place a mechanism to ensure that the transaction request has originated from an "identified device".
- q) Card network shall ensure monitoring to detect any malfunction, anomaly, suspicious behaviour or the presence of unauthorized activity within the tokenisation process and implement a process to alert all stakeholders.
- r) Based on risk perception, etc., card issuers may decide whether to allow cards issued by them to be registered by a token requestor.

Extension of scope of devices for tokenisation

The 2019 Tokenisation Circular provided that the facility of tokenization shall be offered through mobile phones / tablets only. Subsequently, in terms of a circular on "Tokenisation – Card Transactions: Extending the Scope of Permitted Devices", dated August 25, 2021 ("**2021 Tokenisation Circular**"), the scope of tokenisation was extended to include consumer devices – laptops, desktops, wearables (wrist watches, bands, etc.), Internet of Things (IoT) devices, etc.

Framework for Card-on-File Tokenisation

Para 10.4 of the RBI "Guidelines on Regulation of Payment Aggregators and Payment Gateways" dated March 17, 2020 states that PAs shall not store the customer card credentials [also known as Card-on-File ("**CoF**")]] within their database or the server accessed by the merchant. They shall comply with data storage requirements as applicable to Payment System Operators (PSOs).

Taking note of the above restriction on payment aggregators and to enable cardholders to benefit from the security of tokenised card transactions as also the convenience of CoF, the RBI issued a Circular on "Tokenisation - Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services" dated September 7, 2021 ("**CoF Circular 2021**") to extend the device-based tokenisation framework specified in the 2019 Tokenisation Circular and the 2021 Tokenisation Circular, to CoF Tokenisation ("**CoFT**") and to permit card issuers to offer card tokenisation services as Token Service Providers ("**TSPs**").

For the purpose of CoFT, the token shall be unique for every combination of card, token requestor and merchant. In terms of the CoF Circular 2021, the following conditions shall be fulfilled for offering CoFT services:

- a) The facility of tokenization shall be offered by the TSPs only for the cards issued by/ affiliated to them.
- b) The ability to tokenise and de-tokenise card data shall be with the same TSP.
- c) Tokenisation of card data shall be done with explicit customer consent requiring Additional Factor of Authentication (AFA) validation by card issuer.
- d) If card payment for a purchase transaction at a merchant is being performed along with the registration for CoFT, then AFA validation may be combined.
- e) The merchant shall give an option to the cardholder to de-register the token. Further, a token requestor having direct relationship with the cardholder shall list the merchants in respect of whom the CoFT has been opted through it by the cardholder; and provide an option to de-register any such token.
- f) A facility shall also be given by the card issuer to the cardholder to view the list of merchants in respect of whom the CoFT has been opted by her/him, and to de-register any such token. This facility shall be provided through one or more of the following channels – mobile application, internet banking, Interactive Voice Response (IVR) or at branches / offices.
- g) Whenever a card is renewed or replaced, the card issuer shall seek explicit consent of the cardholder for linking it with the merchants with whom (s)he had earlier registered the card.
- h) The TSP shall put in place a mechanism to ensure that the transaction request has originated from the merchant and the token requestor with whom the token is associated.

Further, all other provisions of the 2019 Tokenisation Circular and the 2021 Tokenisation Circular shall be applicable.

Restriction on storage of actual card data and interim measures

The CoF Circular 2021 provided that with effect from January 1, 2022, no entity in the card transaction/payment chain, other than the card issuers and/or card networks, shall store the actual card data. Any such data stored previously shall be purged.

However, this time limit was extended twice by the RBI through its circulars on “Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]” dated December 23, 2021 and June 24, 2022. Finally through its circular dated July 28, 2022 (“**2022 Tokenisation Circular**”), the RBI specified that, with effect from October 1, 2022, no entity in the card transaction/payment chain, other than the card issuers and/or card networks, shall store the actual card data.

Further, for ease of transition to an alternate system in respect of transactions where cardholders decide to enter the card details manually at the time of undertaking the transaction (“**guest checkout transactions**”), the RBI permitted the following as interim measures through the 2022 Tokenisation Circular:

- a) Other than the card issuer and the card network, the merchant or its Payment Aggregator (PA) involved in settlement of such transactions, can save the CoF data for a maximum period of T+4 days (“T” being the transaction date) or till the settlement date, whichever is earlier. This data shall be used only for settlement of such transactions and must be purged thereafter.
- b) For handling other post-transaction activities, acquiring banks can continue to store CoF data until January 31, 2023.

The 2022 Tokenisation Circular categorically states that appropriate penal action, including imposition of business restrictions, shall be considered by the RBI in case of any non-compliance.

Digital Rupee

Section 2(aiv) of the RBI Act, 1934 was amended in 2022 so as to include within the definition of “bank note”, digital currencies or bank notes in digital form. Pursuant to this amendment the Government has started rolling out digital currencies in numerous cities as a part of its pilot project

to adjudge the efficacy of a digitally available currency. The digital rupee has the same legal tender of a rupee of a similar denomination. The design, structure and technology behind the digital rupee has been outlined in the Concept Note on Central Bank Digital Currency published by the RBI on October 7, 2022.

The RBI has divided the digital currency into two main types –

1. The CBDC general purpose (retail) (“**CBDC-R**”), to be used by the private sector and consumers; and
2. CBDC wholesale (“**CBDC-W**”), to be used by banks and settlement systems.

Since the digital rupee shall have full offline functionality, it exposes businesses and the financial system to the risk of double spending by consumers. However the RBI believes this may be mitigated by technical solutions and business rules such as imposing monetary limits on offline transactions. Further, the concept note provides that the impact of the digital rupee may far extend into those similar to smart contracts as the digital rupee may be programmed to be spent only on end-uses for which they are issued. Having a vertical segmentation, the digital rupee would have no single point of failure and use cryptography and quantum resistant algorithms. The RBI also believes that the digital rupee platform shall enable the collection of massive real time data which may help in real time data analysis and uncover money laundering and/or other illegal and fraudulent activities.

Account Aggregators

The legal framework for Account Aggregators (“**AA**”) was issued by the Reserve Bank of India through its Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016 dated September 2, 2016 (“**AA Master Directions**”). The AA Master Directions were issued with the objective of facilitating the aggregation of all financial assets of customers of banks. Financial assets include bank deposits, equity shares, bonds, debentures and insurance policies. The goal was to enable sharing and aggregation of financial data in a secure, transparent and efficient manner. AAs were set up as an intermediary which would also be responsible for managing customers' consent. AAs are required to be registered as an “NBFC - Account Aggregator” with the RBI.

AAs also serve as a data blind consent manager. They act as an intermediary to collect data from Financial Information Providers (“**FIPs**”) such as banks and share such data with Financial Information Users (“**FIUs**”) such as wealth management companies or lending institutions which provide financial services. Any such information is transferred in an encrypted form with the explicit consent of the customer. AAs do not store or use their customers' information.

Since the business of an AA is primarily technology-driven, AAs are required to adopt an IT framework that ensures secure flow of data. Information System Audits of an AAs internal systems shall be conducted at least once in two years by a certified external auditor. AAs, FIU and FIPs are also expected to comply with a set of core technical specifications framed by Reserve Bank Information Technology Private Limited for the participants of the AA ecosystem.

Open Network for Digital Commerce (“**ONDC**”)

ONDC is a Government of India backed initiative, which aims to transform India's e-commerce landscape by creating a pan-India e-commerce platform that connects all Indian buyers and sellers on a single network. The Department for Promotion of Industry and Internal Trade (“**DPIIT**”), under the Ministry of Commerce and Industry, set up a steering committee in November 2020 and an advisory council in July 2021 to provide inputs on the idea of a governmental e-commerce platform. Subsequently, DPIIT issued a strategy paper regarding ONDC in January 2022 and pilot testing for ONDC was kicked off in 5 cities. DPIIT then published its consultation paper in September

2022, outlining the efforts undertaken by it to build trust among buyers and sellers, and invited comments from general public on the same.

ONDC, established as a not-for-profit Company under Section 8 of the Companies Act, 2013, runs as an interoperable network that allows unbundling of the e-commerce value chain. This enables a buyer using one particular e-commerce app to transact with a seller listed on another e-commerce app, as long as both the apps are on the ONDC network, resulting in democratisation of e-commerce.

In simpler terms, ONDC can be understood as one meta store for all e-commerce needs of a consumer across sectors – fashion, food, travel, hotels etc. ONDC will enable the display of products and services from all participating e-commerce platforms in search results across all apps on the network. It allows the consumer to purchase ‘Apple’ the phone, and ‘apple’ the food at the best possible price from one platform, instead of juggling between e-commerce websites such as Amazon, Flipkart, Big Basket and BlinkIt, considering that these apps have synced themselves to the ONDC network.

The open network model envisaged by ONDC transcends the current platform-centric model in which interactions between buyers and sellers are only possible if both parties are users of the same platform or application. Instead, in an open network, buyers and sellers can transact regardless of the platform or application they use to be digitally visible or accessible, as long as they are interoperable.

Currently, ONDC is active in its alpha phase in 181 cities and 2 cities in the beta phase. It has formulated its own network policy (“**ONDC Network Policy**”) which governs the operations of the ONDC network. The ONDC Network Policy, together with the ONDC network participant agreement and the transactional documents (viz. the transaction-level contract executed through the ONDC protocol), constitute the terms of any given transaction on the ONDC network.

The previous edition of the Fintech Primer can be accessed [here](#).

Contributed by:



Vinod Joseph, Partner



Smriti Tripathi, Senior Associate



Anushkaa Shekhar, Associate



Paridhi Jain, Associate



Vasavi Khatri, Associate



Adhip Ray, Associate

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
knowledgecentre@argus-p.com

Mumbai | Delhi | Bengaluru | Kolkata
www.argus-p.com

MUMBAI

11, Free Press House
215, Nariman Point
Mumbai 400021
T: +91 22 6736 2222

DELHI

Express Building
9-10, Bahadurshah Zafar Marg
New Delhi 110002
T: +91 11 2370 1284/5/7

DELHI

155, ESC House, 2nd floor,
Okhla Industrial Estate, Phase 3,
New Delhi – 110020
T: +91 11 45062522

KOLKATA

Binoy Bhavan
3rd Floor, 27B Camac Street
Kolkata 700016
T: +91 33 40650155/56

BENGALURU

68 Nandidurga Road
Jayamahal Extension
Bengaluru 560046
T: +91 80 46462300