FINTECH ROUND-UP 2023-24

FOREWORD

In an era defined by rapid technological advancements and unprecedented digital transformation, the financial sector finds itself at the intersection of innovation and disruption. Fintech, the convergence of finance and technology, has emerged as a catalyst for change, reshaping traditional banking, investment, and payment systems worldwide. In India, a nation renowned for its entrepreneurial zeal and technological prowess, the Fintech revolution is unfolding with remarkable vigour.

As the Fintech landscape in India continues to evolve, so too do the regulatory imperatives that govern its operations. The interplay between innovation and regulation is a delicate razor's edge that requires adept navigation to foster growth while safeguarding against systemic risks and ensuring consumer protection. The regulatory framework must strike a fine balance, encouraging innovation and competition while upholding the integrity and stability of the financial system.

This report offers a bird's eye view on the development of regulations pertaining to Fintech in India in 2023-24, and serves as a compass, guiding practitioners and other stakeholders through the complex maze of regulatory challenges and opportunities. From the burgeoning domain of digital payments to the disruptive potential of digital lending, orienting data practices to blockchain technology, each facet of the Fintech ecosystem is subject to its own unique set of regulatory considerations.

Through rigorous analysis and perceptive insights, this report aims to demystify the regulatory landscape, offering clarity on the evolving frameworks and compliance requirements shaping the Fintech industry in India. It explores the regulatory responses to emerging technologies and business models, highlighting the regulatory gaps, ambiguities, and areas ripe for reform.

Moreover, this report underscores the value of collaboration and dialogue among regulators, industry participants, policymakers, and other stakeholders.

I extend my sincere appreciation to the authors at Khaitan & Co for their dedication and expertise in illuminating this critical subject matter. I trust that their insights will inform industry leaders, investors, and other stakeholders as the industry charts the course for the future of Fintech in India.

Jatinder Handoo
CEO, Digital Lenders Association of India (DLAI)

Harshvardhan Lunia
CEO, Lendingkart
Co-Chair, DLAI Knowledge Committee

Shaily Maheshwari Kajaria
Co-Founder, Tezzract
Co-Chair, DLAI Knowledge Committee

INTRODUCTION

India Inc's tryst with Fintech is slightly over a decade old now. In these ten years, the Fintech ecosystem has grown by leaps and bounds. If one were to go with the official figures, India is poised to become one of the largest digital markets in the world. At 87%, India has the highest Fintech adoption rate among the public compared to the global average of 64%. With this, India has gained the 3rd place in digital payments only after the US and China. These opportunities, along with the favourable ecosystem, create a large growth potential for Fintechs in India.

Significant contributors to the above have been the unprecedented push of the government to the JAM trinity (Jan Dhan Yojana, Aadhaar and Mobile) and India's unique Digital Public Infrastructure built on public-private partnerships. For instance, the infrastructure set up by eKYC, DigiLocker, Aadhaar based authentication, the Account Aggregator Framework, and UPI have been great catalysts for the emergence of various forms of Fintech offerings in credit, payments (both domestic and cross-border), wealth management and other areas. This has also opened investment opportunities, attracting domestic and foreign capital in these areas and fostering the overall economic growth of the country while being true to the core intent of financial inclusion.

As the Fintech ecosystem enters a more nuanced phase, the need for a focused and coordinated approach to regulation by various sectoral regulations has emerged like never before. We can already see the gradual shift in regulators' approaches to the regulation of Fintechs. It has moved on from the early years of mere disclosure-based requirements to light touch and supervision through outsourcing norms, to tight regulations by way of stricter audits, KYC norms, information technology and cyber security frameworks, and finally full-fledged supervision of critical segments like cross-border payments, clamping down on unchecked credit growth, tokenised investments, etc. With the Digital Personal Data Protection Act, 2023 expected to come into force later this year, the interrelationship between Fintechs, regulated entities, and consumers for leveraging personal data will also see a paradigm shift. In summary, the gestation period for those taking regulations lightly is now over. Legal and regulatory compliance, along with strong governance, needs to be on the top agenda for Fintechs and regulated entities alike - not only to safeguard against penal actions but also as a differentiating factor for scaling up and attracting investments.

Khaitan & Co and Digital Lenders Association of India's Fintech Roundup 2023–24 sets out some of the key changes we saw in regulations in the Financial Year 2023-24 that have a direct impact on Fintechs.

Sanjay Khan Nagra
Partner, Khaitan & Co

Smita Jha
Partner, Khaitan & Co

Prashanth Ramdas
Partner, Khaitan & Co

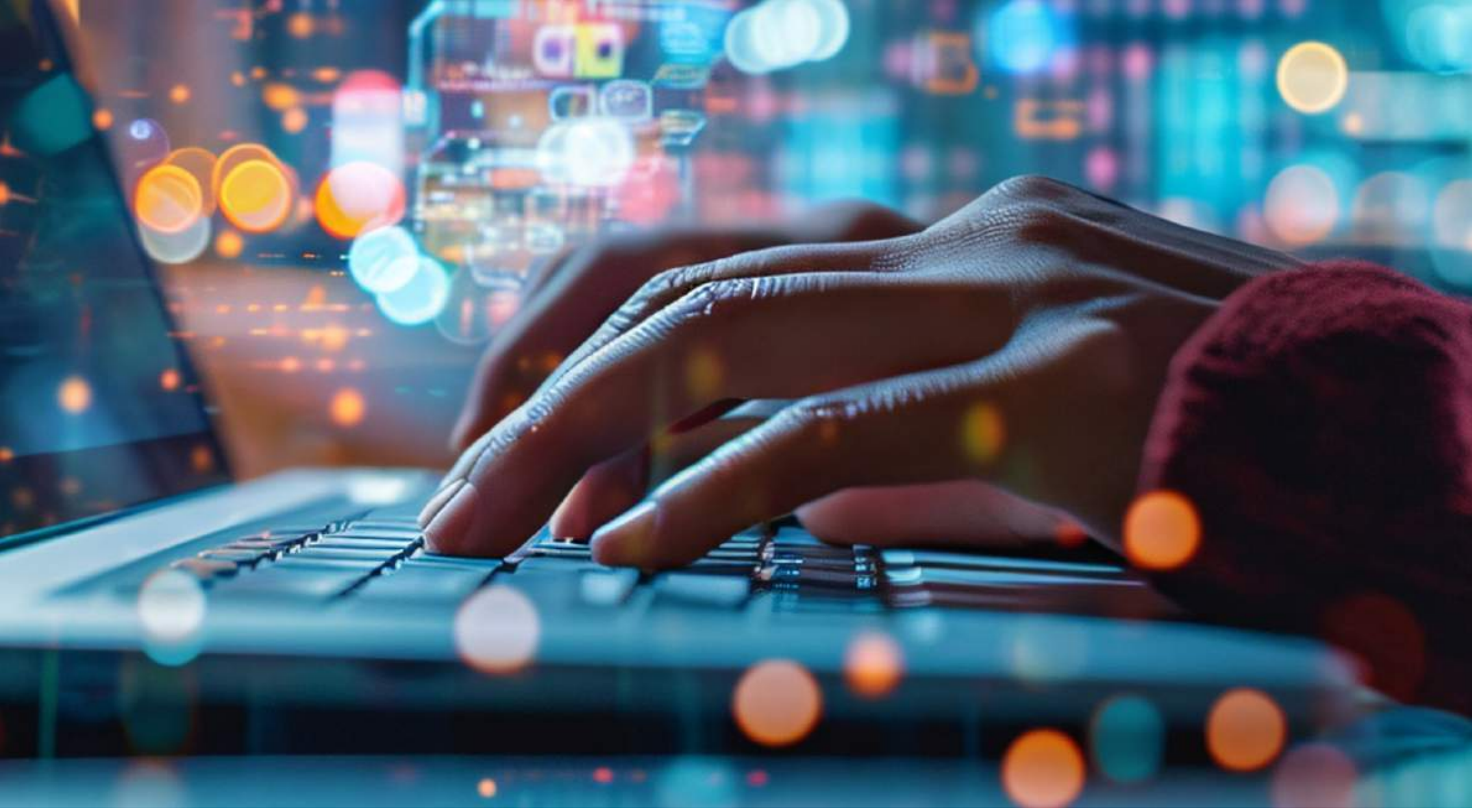


Table of Contents

01

LENDING

Digital lending has been one of the fastest-growing Fintech segments in India. It has seen exponential growth in the last decade. For instance, Fintechs have a larger share of customers who are 'New-to-Credit' or have a credit score below 700.[1] Additionally, approximately 140 million customers were added to the new-to-credit category between the financial year ending in 2019 and that ending in 2022, with 57% of these consumers concentrated in rural and semi-urban areas. Similarly, between the financial year ending in 2017 and that ending in 2020, digital disbursements grew by over 12 times. Further, the buy-now-pay-later (BNPL) segment in India demonstrates a positive trajectory, with its gross merchandise value projected to grow from USD 11.6 billion in 2022 to USD 25.4 billion in 2028.[2]

The systemic vulnerability that a virtual and easily accessible credit flow has created in the market has resulted in the Reserve Bank of India (RBI) adopting a very focused approach to playing a balancing act in catering to the business requirements of Regulated Entities (REs) REs engaged in the digital lending space, protecting consumer rights and interests, and seeking responsible conduct from REs in promoting

[1] *Ernst & Young LLP's report titled 'Unleashing potential – The next phase of digital lending in India' published in September 2023*
[2] *Ernst & Young LLP's report titled 'Unleashing potential – The next phase of digital lending in India' published in September 2023*

unhindered growth of the digital lending segment. In 2023, the measures adopted by the RBI ranged from:

1. Allowing default loss guarantee from unregulated Lending Service Providers (LSPs) to REs upto 5% of the loan portfolios generated by such LSPs
2. Curbing usurious practices adopted by REs in the form of unusually high penal interests
3. Mandating adequate mechanisms for the release of secured properties to safeguard customer interests
4. Setting out special prudential norms for consumer loans and funding of Non-Banking Financial Companies (NBFCs) by banks for such consumer loans
5. Allowing credit lines through Unified Payments Interface (UPI)

We have briefly summarised the key regulatory changes impacting the digital lending ecosystem below:

1. Guidelines on Default Loss Guarantee[3]

The RBI issued the Default Loss Guarantee Guidelines (DLG Guidelines) and provided much-needed legitimacy to DLG (also known as First Loss Default Guarantee or FLDG) arrangements between an RE (such as a bank or NBFC) and Lending Service Providers (LSPs) which are typically unregulated Fintech companies, or *inter-se* REs, with some qualifiers and conditionalities. As a positive development, the RBI modified its stance and clarified that the DLG arrangements falling under its ambit cannot be treated as 'synthetic securitisation' and/or shall also not attract the provisions of 'loan participation'. DLG arrangements have now been permitted under the DLG Guidelines and are subject to the following key conditions:

Applicability

The DLG Guidelines are applicable to arrangements between RE Lenders and DLG Providers which may be LSPs or REs, or between two REs involving DLG. REs and LSPs have the same definition as in the Digital Lending Guidelines,[4] with the additional requirement of being incorporated as a company under the Companies Act 2013 for the DLG Provider. It may be understood from this additional requirement that DLG Providers set up as partnership firms or limited liability partnerships have been prohibited from participating in DLG arrangements.

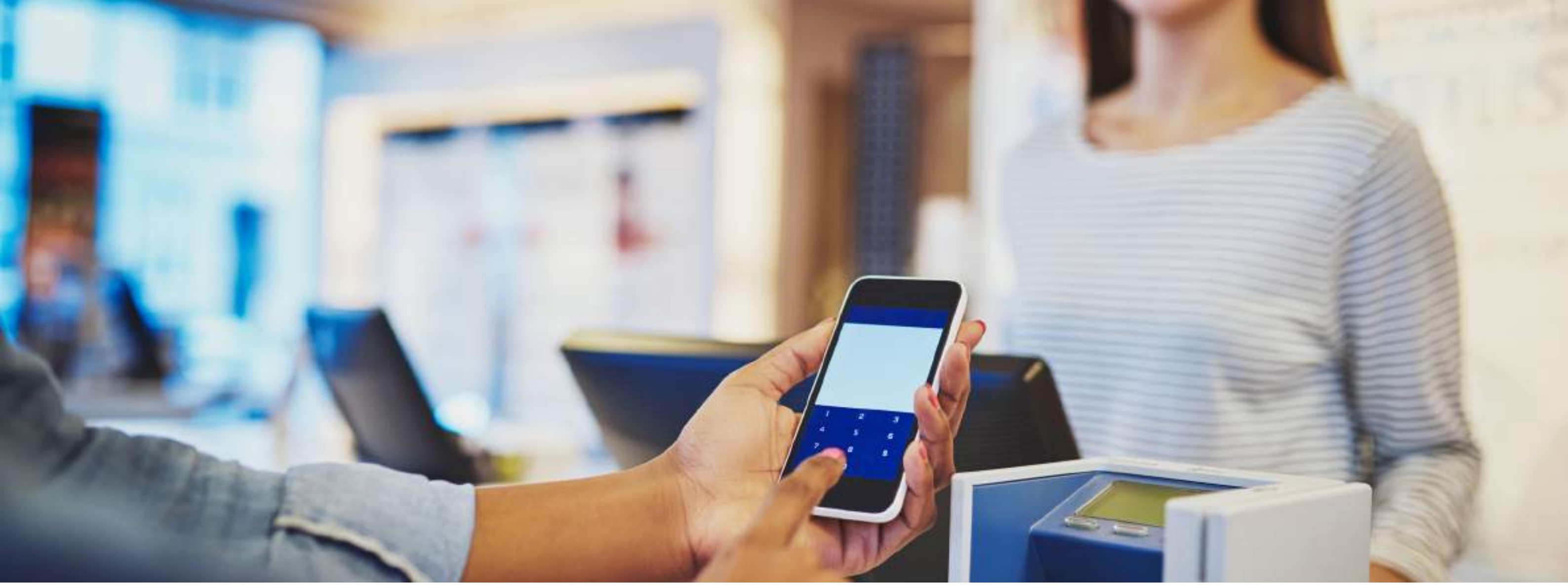
Scope

DLG has been defined as a contractual arrangement between an RE Lender and DLG Provider, under which the DLG Provider guarantees to compensate the RE Lender for a loss due to default up to a certain specified percentage of the loan portfolio of the RE. DLGs would also include any other implicit guarantee of similar nature linked to the performance of the loan portfolio of the RE Lender. Therefore, structures involving performance guarantees and indemnities linked with collections recovery obligations for an underlying portfolio are also intended to be covered by the DLG Guidelines.

Structure of DLG arrangements

DLG arrangements are to be backed by legally enforceable contracts between the RE Lender and DLG Provider, which must, inter alia, cover (i) the extent of DLG cover; (ii) the form of DLG cover to be maintained with the RE; (iii) the timeline for invocation of DLG; and (iv) disclosure requirements

[3] *Reserve Bank of India's circular titled 'Guidelines on Default Loss Guarantee (DLG) in Digital Lending' dated 8 June 2023*
[4] *Reserve Bank of India's circular titled 'Guidelines on Digital Lending' dated 2 September 2022*



including publication (on the RE Lender and DLG Provider's websites) of the total number of portfolios with the amount of each portfolio on which DLG has been offered.

Forms

RE Lenders may only accept DLG in the following forms: (i) cash deposits with the RE; (ii) fixed deposits maintained with a Scheduled Commercial Bank (SCB) with a lien marked in the RE Lender's favor; or (iii) bank guarantee in the RE Lender's favor. This means that structures involving corporate guarantees and risk participation arrangements in the form of contractual indemnities without any funded participation or bank guarantees are not permitted.

Cap on DLG

The total amount of DLG cover on any outstanding portfolio specified upfront cannot exceed 5% of the amount of the loan portfolio in question. This also extends to implicit guarantee arrangements (such as performance indemnities for collections and recoveries as specified above), and the DLG Provider's performance risk cannot exceed 5% of the underlying loan portfolio. The DLG Guidelines are silent on the means and methods of determining the portfolio of loans for the calculation of the 5% cover. While this provides REs with the flexibility to determine their beneficiary portfolios, revolving portfolios may need to be assessed for compliance.

Recognition of non-performing assets

The RE Lender shall be responsible for the recognition of individual loan assets as non-performing assets (NPA) and the consequent provisioning as per the extant asset classification and provisioning norms, irrespective of DLG cover available at the portfolio level. Further, the amount of DLG invoked cannot be set off against the underlying individual loans. Recovery by the RE Lender from the loans on which DLG has been invoked and realised may be shared with the DLG Provider based on the underlying contract with the RE Lender.

Treatment of DLG for regulatory capital

Capital computation of exposure and application of credit risk mitigation benefits on individual loan assets remain governed by the extant norms listed out in the RBI's Master Circular on Basel III Capital Regulation dated 12 May 2023[5] and RBI's Master Directions on Non-Banking Financial Company – Scale Based Regulation, 2023.[6]

[5]Reserve Bank of India's circular titled 'Master Circular – Basel III Capital Regulations' dated 12 May 2023
[6]Reserve Bank of India's circular titled 'Master Direction- Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023' dated 19 October 2023

Tenor

The term of the DLG agreement cannot be less than the term of longest tenor of the loan in the underlying loan portfolio.

Due diligence

RE Lenders must keep the following in mind prior to entering DLG arrangements:

i. RE Lenders shall implement a board approved policy for entering into DLG agreements;
ii. Credit underwriting standards are to be put in place regardless of whether the RE Lender enters into DLG agreements or not;
iii. At the time of entering or renewing a DLG agreement, the RE Lender shall review the DLG Provider's ability to honour the agreement, obtain a declaration to this effect certified by the statutory auditor in relation to the aggregate DLG amount outstanding, and the number of RE Lenders and portfolios against which DLG has been provided (including past default rates on similar portfolios). This may impact competition amongst RE Lenders and DLG Providers.

Customer protection

The RE Lenders shall be required to comply with the instructions on customer protection measures and grievance redressal issues provided in the Digital Lending Guidelines.

Exceptions

The DLG Guidelines exclude the following arrangements and entities from their ambit:

Guarantee schemes of the Credit Guarantee Fund Trust for Micro and Small Enterprises, Credit Risk Guarantee Fund Trust for Low Income Housing and individual schemes under the National Credit Guarantee Trustee Company Ltd.

Credit guarantee provided by the Bank for International Settlements, International Monetary Fund as well as Multilateral Development Banks as referred to in paragraph 5.5 of the RBI Master Circular on Basel III Capital Regulation dated 12 May 2023.

The DLG Guidelines have been applauded for permitting DLG arrangements from LSPs. They provide much-needed clarity and certainty to the digital lending industry and help mitigate systemic risks brought in through the 'rent-an-NBFC' model utilised by certain Fintech companies against which the RBI had raised concerns prior to the Digital Lending Guidelines. Although the ceiling prescribed for the DLG exposure of LSPs is lower than the industry standard and expectations, it is still indicative of the RBI's balancing act of ensuring that the primary responsibility for managing systemic risks remains with REs. The RBI has also taken steps to ensure that REs implement appropriate safeguards, such as board-approved policies and customer protection measures.

As a financial sector regulator, the RBI has attempted to tighten the screws on certain opportunistic arbitrage to ensure that the digital lending ecosystem remains transparently managed and insulated against various risks.

2. Pre-sanctioned credit lines through UPI

With a view of facilitating increased penetration of credit lines across different customer segments, the RBI indicated through its press release dated 6 April 2023[7] the intention to leverage the reach of the UPI network by integrating credit lines into UPI. The intention was also to simplify credit transactions and provide a quicker avenue for accessing credit lines. Following this, the RBI issued the UPI Credit Lines Circular[8] allowing the pre-sanctioned credit line of a bank to be used as a funding account for enabling payments through UPI. The UPI Credit Lines Circular enables banks to offer all types of credit facilities through UPI, including credit lines, in addition to the already available linking of UPI with savings accounts, overdraft accounts, prepaid wallets, and RuPay credit cards.

Banks may introduce credit lines on the UPI platform only with the prior explicit consent of the individual customer. Further, banks may stipulate the terms and conditions of such credit line offerings (such as rate of interest, credit limit, period of credit, etc.) as per their board approved policy. This facility allows for seamless linking of the pre-sanctioned credit line account from the issuer bank to the existing UPI platform through just the registered phone number. The facility can currently be used to make payments to only merchants through QR codes and on e-commerce platforms. Notably, the UPI Credit Lines Circular allows only pre-sanctioned credit lines offered by banks to be linked to the UPI ecosystem; the functionality is yet to be extended to NBFCs. Currently, Axis Bank, HDFC Bank, ICICI Bank, Punjab National Bank and State Bank of India are offering the function of linking their credit lines to UPI.

3. Penal Interest Circular[9] and clarifications

Traditionally, lenders have been allowed to determine their own policies in connection with penal charges and interests applicable to loan accounts in line with the broad guidelines prescribed by the RBI in this regard. However, due to many lenders utilising such penal charges and interests as revenue enhancement tools over and above the contracted interest rate (especially in digital lending segment), the RBI, through the Penal Interest Circular and the subsequent circular dated 29 December 2023[10] (for extending the effective date of the Penal Interest Circular) and the FAQs dated 15 January 2024,[11] issued instructions to REs, to ensure reasonableness and transparency in the levy of penalties in their lending practices.

The Penal Interest Circular, effective 1 April 2024, aims to ensure that the levy of penalties on loan accounts is only to inculcate a sense of credit discipline among borrowers through negative incentives and ensure fair compensation to REs. To this end, the RBI has distinguished between 'penal charge'

---

[7] *Reserve Bank of India's press release titled 'Statement on Developmental and Regulatory Policies' dated 6 April 2024*
[8] *Reserve Bank of India's circular titled 'Operation of Pre-Sanctioned Credit Lines at Banks through Unified Payments Interface (UPI)' dated 4 September 2023*
[9] *Reserve Bank of India's circular titled 'Fair Lending Practice – Penal Charges in Loan Accounts' dated 18 August 2023*
[10] *Reserve Bank of India's circular titled 'Fair Lending Practice - Penal Charges in Loan Accounts: Extension of Timeline for Implementation of Instructions' dated 29 December 2023*
[11] *Reserve Bank of India's FAQs in connection with Fair Lending Practice - Penal Charges in Loan Accounts dated 15 January 2024*

and 'penal interest' (charged above and beyond the interest rate and then capitalised) and permitted the former to be levied as a pre-determined amount or rate notified to the borrower prior to or at the time of sanction of the loan, as opposed to the widely practiced levy of 'penal interest' above and beyond the interest charged on the loan. The penal charges cannot be compounded, and in the event of a payment default, they are required to be levied only on the defaulted amounts and not on all outstanding amounts. However, the FAQs have clarified that REs may still charge interest on unpaid interest (including on unpaid EMI) at the contracted rate of interest until the date of remediation, but not at the penal rate of interest.

Additionally, it has been specifically clarified that the penal charges for loans sanctioned to individual borrowers for purposes other than business, should not be higher than for non-individual borrowers for similar non-compliance with material terms. This specifically impacts the consumer finance segment of digital lending, which is traditionally known for levying higher penal interests. This ensures that individual customers also benefit from the market rates for business entities who have better negotiating prowess in matters of credit.

Further, the RBI has, as an additional layer of catch-all protection, clarified that no additional components should be introduced to calculate a borrower's rate of interest in relation to a breach of material terms of the loan agreement by the borrower. Simply put, penal charges for non-compliance with the material terms of the loan agreement should be fair and consistent for all borrowers in the same category of loan / product. However, it was clarified through the FAQs that REs may charge different penalties within the same product category depending on the loan amount, provided they adopt a suitable structure of penal charges that is 'reasonable' and 'commensurate' with the non-compliance of material terms of the loan agreement.

The Penal Interest Circular requires REs to disclose the rationale for penal charges in the loan agreement, the most important terms and conditions and key facts statement (as applicable), and on the RE's website under the specific heading 'Interest Rates and Service Charges'. The REs must also communicate to the borrowers the applicable penalty and reason for it at the time of levying it, as well as furnish reminders for non-compliance with the material terms of the loan agreement.

4. Responsible lending practice around release of security

The RBI's fair practice code issued to REs mandates that REs release all securities when the borrower repays the outstanding amounts. However, due to disparate methods adopted by the REs in releasing security documents upon closure of loan accounts, the RBI issued the Secured Assets Directions[12] to regulate and provide clarity on the release of secured assets.

The Secured Assets Directions apply to personal loans given to individuals and include (i) consumer credit; (ii) education loans; (iii) loans given for the creation or enhancement of the immovable assets; and (iv) loans given for investment in financial assets. The secured assets must be released along with any associated charges within 30 days of full repayment of the due amount. Further, the Secured Assets Directions require lenders to provide the borrower with the option to collect the secured assets either from the loan servicing branch or any other office of the lender where the documents are available. In case of delay in release of secured assets that may be attributable to the lender or loss of or damage to the secured assets, the borrower is entitled to a compensation of INR 5,000 (~USD 60) for each day. Further, the lender will be required to assist the borrower in obtaining duplicates or certified copies of the lost or damaged secured assets at their own expense. However, an additional 30 days will be available to the lender, and the delay penalty will be calculated after a total period of 60 days.

REs are required to provide certain upfront clarifications and information to the borrower for their benefit. REs are also required to mention the timeline for return of the secured assets in the sanction letter and clearly set out the procedure on their website for return of the secured assets to the borrower's heir in case of the borrower's demise.

5. Consumer loan prudential norms

The RBI issued the Consumer Loan Circular[13] to REs to increase the risk weightage in relation to (i) REs' consumer credit exposure; and (ii) banks' credit to NBFCs. It was observed by the RBI that there had been high and reasonably unchecked growth in consumer credit and the dependency of NBFCs on bank borrowings in recent years. To counterbalance the growth of this segment against the systemic risk posed, the Consumer Loan Circular sets out the following directions in relation to consumer credit exposure and bank credit to NBFCs:

Consumer credit exposure

i. **Banks**: The risk weight in respect of outstanding and new consumer credit exposure of commercial banks, including personal loans, has been increased from 100% to 125%. However, the RBI has provided a specific exemption for housing loans, education loans, vehicle loans, and loans secured by gold and gold jewellery.

ii. **NBFCs:** The risk weight in terms of outstanding and new consumer credit exposure of NBFCs categorised as retail loans has been increased from 100% to 125%. However, the RBI has provided a specific exemption for housing loans, educational loans, vehicle loans, loans against gold jewellery and microfinance / SHG loans.

[12]*Reserve Bank of India's circular titled 'Responsible Lending Conduct – Release of Movable / Immovable Property Documents on Repayment/ Settlement of Personal Loans' dated 13 September 2023*

[13]*Reserve Bank of India's circular titled 'Regulatory measures towards consumer credit and bank credit to NBFCs' dated 16 November 2023 dated 16 November 2023*

iii. **Credit card receivables:** The risk weight for credit card receivables has been increased from 125% to 150% for SCBs and from 100% to 125% for NBFCs.

Bank credit to NBFCs

i. **SCBs:** Prior to the publication of the Consumer Loan Circular, the risk exposures of SCBs to NBFCs were assigned risk weightage as per the ratings assigned by accredited external credit assessment institutions. To this end, the RBI has increased the risk weights on such exposures of SCBs by 25 percentage points (over and above the risk weight associated with the given external rating) where the extant risk weight as per the external rating of NBFCs is below 100%.

ii. **Exclusions:** The RBI has excluded loans to HFCs and loans to NBFCs classified as priority sector lending (such as microfinance and micro, small and medium enterprises (MSME) lending) from this instruction.

REs are required to, at the earliest, but in any event by 29 February 2024, review their extant sectoral exposure limits for consumer credit and adopt board approved limits for various sub-segments under consumer credit (including all unsecured consumer credit exposures) as part of their risk management framework. This must include strict adherence to the approved limits and a mechanism for continuous monitoring of the same by the risk management committee. Specifically, top-up loans extended by REs against depreciating movable assets (such as vehicles), must be treated as unsecured loans for credit appraisal, prudential limits and exposure purposes, with immediate effect.

02

PAYMENTS

The financial year 2023-24 has been a watershed year for the Indian payments industry. At the G20 Summit in September 2023, the Government of India showcased the prowess of India's digital payments infrastructure. As of January 2024, India witnessed 210,288.7 billion digital payments transactions.[1] With this unprecedented success, the National Payments Corporation of Indian (NPCI) released various circulars on revising its existing framework on UPI and e-Mandates with the objective of making UPI a global product, showcasing India's vast progress made in digital payments in a short span of time. Initiatives such as permitting Non-Resident Indians (NRIs) to access the UPI framework and collaborations with nations such as Singapore, the United Kingdom, France, Bhutan, Nepal and the United Arab Emirates for setting up the UPI infrastructure would lead to many other future use cases of the UPI infrastructure.

Recognising the need for increasing the accessibility and adequacy of the UPI framework amongst various sections of society, NPCI launched various features such as increases in UPI transaction limits, voice-enabled Hello UPI, Near Field Communication (NFC) enabled UPI Lite X and UPI Tap and Pay. However, the NPCI also cautioned the industry regarding the usage of UPI rails only by authorised institutions by clarifying the ban on the usage of UPI rails by unregulated entities for issuing look-alike products. It also revisited its existing regulatory framework on e-Mandate frameworks.

[1] *Reserve Bank of India, 'Payment System Indicators – January 2024'*

The year 2023 was also marked by grant of payment aggregator licenses by the RBI. Leveraging on existing payment aggregation capabilities, the RBI also took a step forward towards overhauling the regulatory framework for cross-border payments for import-export transactions and mandated the introduction of various new payment methods to increase the accessibility of digital payments in India. The RBI categorised entities providing payment aggregation services for cross-border transactions (such as online payment gateway service providers (OPGSPs) and collection agents) on similar regulatory footing to the existing payment aggregation regulatory framework for domestic transactions by introducing the PA-CB Guidelines.[2] Through the PA-CB Guidelines, the RBI addressed concerns related to low transaction limits and operational hurdles in implementing cross-border payment arrangements under the erstwhile regulatory regime. PA-CBs are mandatorily required to register with the Financial Intelligence Unit - India (FIU-IND), which put to rest the regulatory uncertainty arising out of the view taken by the hon'ble Delhi High Court in the PayPal Judgement.[3]

Most recently, the RBI has created a stir with regulatory action against a certain unnamed card network permitting business payment solution providers (BPSP) to operate an unauthorised payment system in violation of the Payments and Settlement System Act (PSS Act).[4] Intermediaries offering payment solutions must now re-look at their models and assess the need for regulatory licensing for the same.

The RBI also revised the regulatory framework for BBPS, also understood as an 'anytime anywhere' bill payments platform, with the intention to (i) include all categories of payments and collections, both recurring and non-recurring in nature, as well as facilitate inbound cross-border bill payments; and (ii) enhance the efficiency of the system and also encourage greater participation. The new regulatory framework seeks to streamline the process flow of transactions and membership criteria for onboarding operating units in BBPS.

With the close of an eventful year for the payments sector, India is set to enter a year where it not just keeps pace with but leads the charge into a dynamic and transformative future of payments, with consolidation and streamlining of its payment products as well as the overall regulatory regime.

[2]RBI circular on 'Regulation of Payment Aggregator – Cross Border (PA – Cross Border)' dated 31 October 2023.
[3]PayPal Payments v Financial Intelligence Unit India, 2023 SCC OnLine Del 4336
[4]Payment and Settlement Systems Act 2007, Act No. 51 of 2007

We have briefly summarised below the recent and most significant developments in the payments industry over the last year:

1. Delhi High Court's judgement on OPGSPs

On 24 July 2023, the Hon'ble Delhi High Court in the PayPal judgement held that (OPGSPs) would fall within the definition of a payment system operator (PSO) for the purpose of the Prevention of Money Laundering Act (PMLA).[5] Accordingly, OPGSPs were classified as 'reporting entities' under the PMLA. We have briefly summarised the key take-aways from the PayPal judgement as follows:

Categorisation of OPGSPs as 'reporting entities' under PMLA

The court held that even though OPGSPs are not categorised as PSOs under the PSS Act, they would be categorised as PSOs for the purposes of PMLA and would be considered reporting entities. As part of the judgement, the hon'ble court did not agree that the definition of 'payment system' under both legislations is similar and further distinguished the objective of the PSS Act from that of PMLA. While the former seeks to primarily regulate entities that are involved in the handling of funds (such as payment aggregators), the latter seeks to primarily mitigate risks associated with money laundering and terrorism financing and accordingly imposes various reporting obligations on REs in relation to data collection and analysis.

Distinction made with TPAPs

The court distinguished between the activities performed by OPGSPs as compared to those of third party application providers (TPAP) in the UPI ecosystem primarily based on the following parameters:

1

TPAPs participate in UPI, wherein remitters as well as the beneficiaries are required to register themselves with payment service provider (PSP) banks, and all the details relating to transactions processed in the UPI ecosystem (including the details of the remitters and the beneficiaries) are available with the PSP Banks, which are themselves reporting entities.

2

In contrast, for cross-border payments facilitated by OPGSPs through authorised dealer (AD) banks, the AD Banks may not have all the details relating to such payments (such as the details of the remitters for export transactions).

3

Based on this, the court held that TPAPs would not be categorised as PSOs under PMLA and resultantly, would not need to adhere to obligations imposed on reporting entities under PMLA.

[5] *Prevention of Money Laundering Act 2002, Act No. 15 of 2003*

Implications

The PayPal judgement laid down that actual handling of funds cannot be a decisive factor in determining whether a payment intermediary would be categorised as a PSO (and resultantly, an RE) under PMLA.

However, the PayPal judgement was passed by a single judge bench of the Delhi High Court and is currently under appeal before a division bench of the Delhi High Court. Moreover, now that the RBI has brought entities undertaking activities of the erstwhile OPGSPs under the ambit of the PA-CB Guidelines, they have been statutorily mandated to be registered as reporting entity under the PMLA. Therefore, the outcome of the appeal is not likely to have any impact on the industry other than the party contesting the penalties imposed by the FIU-IND.

2. Guidelines for regulation of payment aggregators – Cross-border

On 31 October 2023, the RBI issued the PA-CB Guidelines, marking a significant and long-awaited departure from the existing regulatory framework for cross-border payment transactions. The PA-CB Guidelines would apply to all entities involved in facilitating cross-border payment transactions for the import and export of goods and services. We have briefly summarised the key highlights and deviations from the erstwhile regulatory framework below:

Consolidated regulatory framework

Before the PA-CB Guidelines, non-bank entities facilitating cross-border payments were categorised as OPGSP and 'collection agents'. Under the PA-CB Guidelines, a comprehensive definition of a PA-CB includes both OPGSPs and collection agents. This results in direct regulatory supervision by the RBI, a departure from the erstwhile indirect oversight through AD Banks.

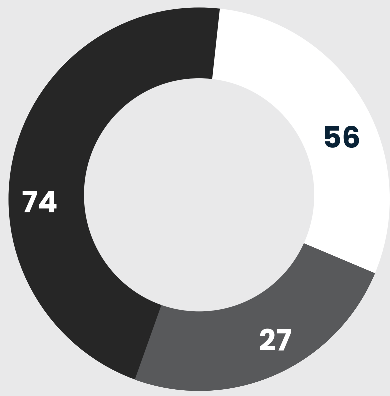
Registration requirements

Non-bank entities providing or intending to provide PA-CB services, including OPGSPs and collection agents, must apply for authorisation with the RBI by 30 April 2024. Existing PA-CBs need to register with the FIU-IND before seeking authorization. This aligns with the RBI's goal of direct regulation for entities involved in cross-border trade transactions.

Immediate compliance requirements

Existing PA-CBs must comply with specific aspects of the PA Guidelines by 31 January 2024. This includes governance standards, merchant onboarding policies, customer grievance redressal frameworks, baseline technology requirements and security protocols. Failure to comply may result in license application being refused.

Status of domestic payment aggregators applications	No. of applicants
Authorised online PAs	17
Existing PAs with in-principal authorisation	32
Existing PAs whose applications are under process	6
Existing PAs whose application was returned (pending re-application)	1
New PAs who have received in-principal authorisation	17
New PAs whose applications are under process	10
Existing PAs whose applications were returned / withdrawn / refused	25
New PAs whose applications were returned / withdrawn / refused	49



Can operate ■ Cannot operate until authorised ■ Cannot operate - authorisation denied

Source: RBI

Minimum capitalization norms

Applicant entities must have an initial net worth of INR 15,00,00,000 (~USD 1,800,000), increasing to INR 25,00,00,000 (~USD 3,000,000) within three years. Existing PA–CBs failing to meet net worth requirements or apply for authorization by 30 April 2024 must wind up operations by 31 July 2024.

Transaction limits

PA-CBs can process payments for import and export transactions up to a maximum per unit value of goods/services of INR 25,00,000 (~USD 30,000). This is a notable increase from previous limits under the OPGSP regime (i.e., USD 2,000 per import transaction and USD 10,000 per export transaction), allowing more flexibility and greater volumes for cross-border trade transactions.

Transaction sourcing and merchant due diligence

PA-CBs must conduct due diligence on merchants, e-commerce marketplaces, and payment aggregators. They are responsible for ensuring compliance with India's foreign trade policy and adherence to the Know Your Customer (KYC) Master Directions.[6]

Fund flows for import and export transactions

PA-CBs facilitating import transactions must maintain an Import Collection Account (ICA) with an AD Bank. For export transactions, an Export Collection Account (ECA) is required. The prescribed fund flows must align with the PA Guidelines,[7] providing a degree of flexibility in settlement timelines.

FEMA reporting requirements

AD Banks maintaining ICA/ECA for PA-CBs must ensure compliance with Indian exchange control regulations for underlying trade transactions, including reporting and reconciliation on Export Data Processing and Monitoring System (EDPMS) and Import Data Processing and Monitoring System (IDPMS).

In conclusion, the PA-CB Guidelines mark a pivotal moment in the liberalisation of the regulatory

[6] *RBI's circular titled 'Master Direction- Know Your Customer (KYC) Direction, 2016' dated 25 February 2016*
[7] *RBI's circular titled 'Guidelines on Regulation of Payment Aggregators and Payment Gateways' dated 17 March 2020*

framework for cross-border payments. The regulatory shift brings operational flexibility to entities engaged in facilitating trade transactions, emphasising the need for robust compliance. By directly regulating PA-CBs, the RBI aims to streamline and enhance the efficiency of cross-border payment processes, providing a regulatory landscape that fosters both innovation and adherence to stringent standards. This forward-looking approach sets the stage for a new era in cross-border payments, enabling seamless and compliant trade transactions for all stakeholders involved.

3. Charges on UPI linked PPIs merchant transactions

On 24 March 2023, the NPCI introduced certain charges on merchant transactions initiated using Prepaid Payment Instruments (PPIs) on UPI. Such charges include the following:

Interchange

1.1% of the transaction value will be applied as interchange fee to all online merchants, large merchants, and small offline merchants with a transaction value greater than INR 2,000 (~USD 24).

For industry programme merchant category codes, the following interchange will apply:

Telecom
0.70%

Convenience Store
1.10%

Mutual Fund
1% on transaction value by acquirer to Issuer capped at INR 15

Education
0.70% on transaction value by acquirer to Issuer capped at INR 15

Insurance
1% on transaction value by acquirer to Issuer capped at INR 10

Government Services
1% on transaction value by acquirer to Issuer capped at INR 10

Wallet loading service charge

PPI issuers are required to pay 15 basis points as a wallet loading service charge to the remitter bank for loading transaction value greater than INR 2,000 (~USD 24).

The above-mentioned interchange fee will not be applicable on peer-to-peer and P2PM, i.e., small merchants with monthly inward UPI transactions up to INR 50,000 (~USD 600) transactions between bank accounts and PPI wallets.

4. Restriction on accessing UPI rails by co-branded PPI apps/partner

The PPI Master Directions[8] mandated PPI issuers issuing full KYC PPI wallets facilitate access to UPI functions for PPI holders. The PPI Master Directions also stipulate that PPI holders can be onboarded for UPI by authorised PPI issuers only. Taking cognizance of the prevailing market practices, NPCI directed all PPI issuers to discontinue access to UPI rails for customers of its co-branded partners.

[8]*Reserve Bank of India's circular titled 'Master Directions on Prepaid Payment Instruments (PPIs)' dated 27 August 2021*

5. Framework relating to offline digital payments

The RBI, through its Statement on Developmental and Regulatory Policies dated 10 August 2023,[9] introduced directives aimed at enhancing offline payments. With a focus on expediting small-value transactions and facilitating seamless digital payments in areas with limited internet or telecom connectivity, the following measures were announced:

Offline payments on UPI

To streamline and expedite small-value transactions on UPI, the RBI launched the UPI-Lite wallet in September 2022. The RBI stated that the promotion of UPI-Lite involves facilitating offline transactions through NFC technology. Further to this statement, the RBI governor announced, 'UPI Lite X', which is a feature that allows users to both send and receive money without internet connectivity through NFC technology. This feature aims to empower retail digital payments in scenarios where internet or telecom connectivity is weak or unavailable and ensure minimal transaction declines.

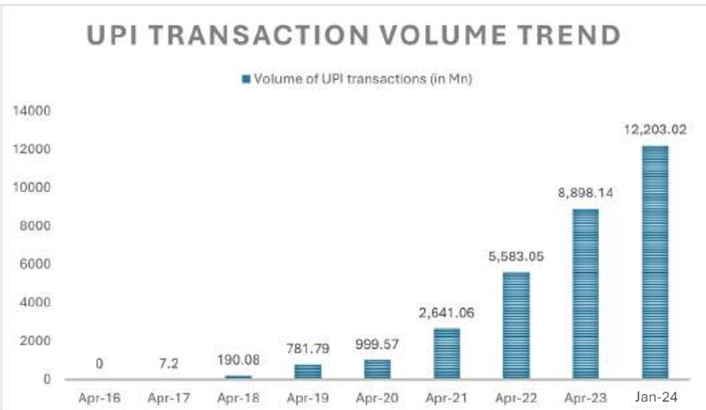
Enhancing transaction limits for small value digital payments

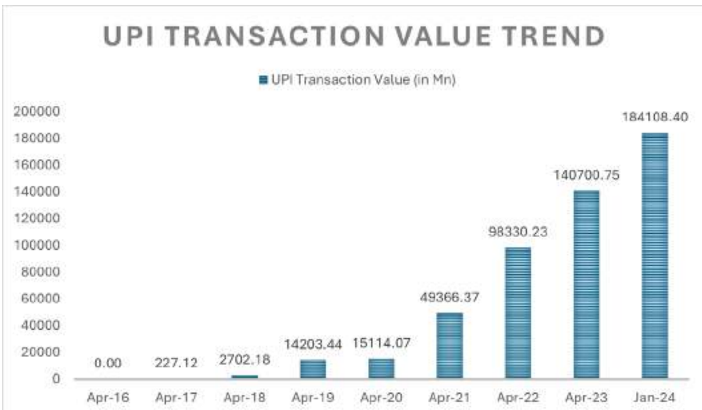
The RBI has revised the existing transaction limits of INR 200 (~USD 2.4) per transaction for small value digital payments in offline mode to INR 500 (~USD 6) per transaction. This enhancement aims to facilitate faster, more reliable, and contactless payments for everyday transactions, transit payments and more. It is crucial to note that, despite the increase in per transaction limits, the overall limit remains at INR 2,000 (~USD 24). The RBI formalised this directive by issuing a notification,[10] which was implemented by the NPCI on 31 August 2023.

6. UPI Tap & Pay

On 19 December 2023, the NPCI issued a circular to enable the 'Tap & Pay' feature on UPI[11] and mandated TPAPs to implement the Tap & Pay feature on their applications.

UPI applications can provide the Tap & Pay feature only on mobile devices equipped with NFC. NPCI mandates that the UPI application must obtain prior permission from the customer before enabling NFC on their devices to carry out Tap & Pay transactions. For UPI LITE, transactions below INR 500 (~USD 6) may be processed without a PIN.





[9] *Reserve Bank of India's 'Statement on Developmental and Regulatory Policies' dated 10 Agusut 2023*
[10] *Reserve Bank of India's notification titled 'Enhancing transaction limits for Small Value Digital Payments in Offline Mode' dated 24 August 2024*
[11] *National Payments Corporation of India's circular titled 'Introduction of UPI TAP & PAY mode of payments' dated 19 December 2023*

7. Enhancement of transaction and e-Mandate limits

The RBI through its Statement on Developmental and Regulatory Policies announced several changes to boost the financial ecosystem on 8 December 2023.[12] Some of the key initiatives under the statement include:

Enhancement of UPI limits for specific categories

The per-transaction limits for UPI payments have been enhanced from INR 1,00,000 (~USD 1,200) to INR 5,00,000 (~USD 6,000) for hospitals and educational institutions.[13]

Simplification of e-Mandates and harmonisation of limits

The NPCI, on 21 July 2023, simplified e-Mandate registration through the e-Mandate Circular.[14] The e-Mandate Circular also revises the limits of different forms of mandates.

Simplification of e-Mandates: An e-Mandate can now be authenticated through any one of the following values, followed by a one-time password authentication by the bank:

- Last four digits of Aadhaar number of the customer
- Last five digits of PAN of the customer
- Customer ID, as provided to the customer by their respective banks

The limit for e-Mandates registered through the present simplified process will be up to INR 15,000 (~USD 180). However, security mandates cannot be registered through the present mechanism.

Harmonisation of mandate limits: The e-Mandate Circular also allowed for the mandate amount limit for all electronic variants to be enhanced in order to be at par with the current limit of INR 1,00,00,000 (~USD 120,700) for physical mandates.

Expansion of existing e-Mandate limits: The limit for executing e-Mandates without AFA was revised from INR 15,000 (~USD 180) to INR 1,00,000 (~USD 1,200). This exemption has been granted for specific categories like mutual fund subscriptions, insurance premium payments, and credit card settlements.

8. Penalty for a high percentage of debit returns

On 18 August 2023, the NPCI notified the Penalty Circular,[15] which laid down the following instructions:

i. Returned transactions can only be re-presented twice after the return of the initial presentation.
ii. Re-presentation of a returned transaction can only be done three days after the date of return of the automatic clearing house (ACH) presentation.
iii. Re-presentation can only be done after confirmation from the customer on the availability of the appropriate balance in the customer's bank account.
iv. For repeated returns, destination banks should monitor the operation of the customer's bank account and advise the customer to maintain a sufficient balance in their associated bank account.

[12] *Reserve Bank of India's 'Statement on Developmental and Regulatory Policies' dated 8 December 2023*
[13] *National Payments Corporation of India's circular titled 'Implementation of Rs 5 Lakh Limit per transaction for specific categories in UPI' dated 19 December 2023*
[14] *National Payments Corporation of India's circular titled 'E-Mandate simplification and harmonization of the limit of all variants of mandates' dated 21 July 2023*
[15] *National Payments Corporation of India's circular titled 'Penalty for high %age of ACH debit returns' dated 18 August 2023*

Further, to address the high percentages of return ACH mandates, the NPCI would levy penalties on corporate users with return ACH mandates above 50%. The NPCI also mandated barring corporate users from registering new mandates in case the return ACH mandates exceeded 30% by 1 April 2024.

9. Standardisation of the duration of NACH mandates

NPCI, vide circular 18 August 2023[16] mandated compliance with following durations for the issuance of National Automated Clearing House (NACH) mandates:

i. A NACH mandate may be issued for any duration up to 30 years from its issuance. The NPCI's central NACH system will only accept mandates for durations of 30 years or less.
ii. A NACH mandate must also provide the 'Final collection date' or end date for all categories of mandates going forward. To this end, the option of 'until cancelled' has been removed.
iii. A0001 (API Mandate) category code has been discontinued, and members have been directed to present the mandate with appropriate category codes as far as possible.

10. Restraining BPSP arrangements

On 15 February 2024, the RBI issued a press release[17] through which it identified arrangements involving card networks facilitating businesses to make card payments through intermediaries to entities that do not accept card payments. In this arrangement, the intermediary was collecting card payments from corporations for commercial transactions and then transferring the funds to non-card accepting recipients via IMPS / RTGS / NEFT. This arrangement is commonly referred to as BPSP in market terminology.

On examination, the RBI classified BPSP arrangements in the nature of a 'payment system' under the PSS Act. It noted that necessary authorisation under the PSS Act had not been obtained, rendering this an unauthorised activity. It also noted concerns stemming from the fact that the intermediary pooled large sums of funds into an account not designated under the PSS Act; and the transactions processed through this arrangement failed to comply with the originator and beneficiary information requirements outlined in the KYC Master Directions.

The RBI has advised the unnamed card network to suspend such arrangements until further notice. The RBI also emphasised that this action does not aim to restrict the normal usage of business credit cards.

11. Reserve Bank of India (Bharat Bill Payment System) Directions, 2024

RBI issued the BBPS Directions[18] superseding the erstwhile guidelines in relation to BBPS. BBPS is an integrated bill payment platform that enables payment / collection of bills through multiple channels (mobile apps, mobile banking, physical agents, bank branches, etc.) using various payment modes (UPI, internet banking, cards, cash, prepaid payment instruments, etc.). The transactions facilitated through this platform will require the bill to be fetched before payment initiation. In the case of transactions involving payments for prepaid services, the customer relationship with the biller will be validated through the platform.

---

[16] *National Payments Corporation of India's circular titled 'Mandate duration and mandatory final collection date' dated 18 August 2023*
[17] *Reserve Bank of India's press release titled 'Payment Intermediary by Card Network – Restraining of Unauthorized Payment System' dated 15 February 2024*
[18] *Reserve Bank of India's circular titled 'Reserve Bank of India (Bharat Bill Payment System) Directions, 2024' dated 29 February 2024*

We have briefly summarised the key changes introduced under the BBPS Directions as follows:

Applicability

The BBPS Directions apply to NPCI Bharat Bill Pay Limited (NBBL), Bharat Bill Pay Central Unit (BBPCU), Bharat Bill Payment Operating Unit (BBPOU) and agent institutions certified by NBBL to provide customer interface for bill payments.

Definitions

The BBPS Directions has made amendment to the existing definitions of BBPS, BBPCU and BBPOU to provide clarifications. The BBPS Directions also provides new definitions of Biller Operating Unit (BOU), Customer Operating Unit (COU), Agent Institutions, Biller Aggregator and TSPs:

i. **Bill:** The definition of bill now also includes notice or advice for the recharge of prepaid services.
ii. **BBPS:** BBPS has now been described as an 'integrated bill payment' platform as opposed to its earlier definition of 'integrated bill system' which enables payment / collection of bills through multiple channels and using various payment modes. The definition now also includes aspects related to transactions facilitated through the BBPS platform and the fetching of a customer's bill for payment initiation. For transactions involving payments for prepaid services, the customer relationship with the biller is validated through the platform.
iii. **BBPCU:** As previously provided for under erstwhile guidelines, under the BBPS Guidelines, BBPCU is the governing body responsible for overseeing BBPS operations. It establishes operational, technical, and business standards, and manages clearing and settlement functions. NBBL, in its capacity as a BBPCU, has been authorised to act as a payment system provider for BBPS.
iv. **BBPOU:** A BBPOU is now defined as a system participant and can function either as a BOU or COU.
v. **BOU:** A BBPOU responsible for onboarding billers onto the BBPS platform, either directly or through Biller Aggregators, to facilitate bill collection.
vi. **COU:** An entity providing a physical/digital interface for facilitating bills, either directly or through agent institution(s).
vii. **Agent institution:** Entities certified by NBBL that provide a customer interface, whether physical or digital for bill payments.
viii. **Biller Aggregator:** An entity that aggregates billers for the purpose of enabling them to connect to a BOU.
ix. **TSP:** Entities certified by NBBL to provide technology services and solutions enabling billers, BBPOUs or Agent Institutions to integrate with BBPS.

Authorisation requirements

i

Any entity, other than a biller, operating a bill payment system beyond the purview of BBPS would fall within the ambit of a 'payment system' and will require authorisation to undertake such activity.

ii

Bank and non-bank payment aggregators, intending to operate as a BBPOU do not require separate authorisation and only need to intimate RBI before commencing its operations.

iii

The BBPS Directions also mandate agent institutions to obtain certification from NBBL for conducting their activities.

Roles and responsibilities of BBPCU

The BBPS Directions set out the following indicative roles and responsibilities for BBPCU:

i. Setting the rules and regulations, technical standards for governing participation criteria and system operations in BBPS.
ii. Providing guaranteed settlement of all transactions routed through NBBL.
iii. Ensuring that all transactions have BBPS reference number from the payment initiation stage.
iv. Ensuring no funds in the system flow through any TSP.
v. Providing a framework for the redressal of consumer disputes.

Roles and responsibilities of BOU

The BBPS Directions set out the following indicative roles and responsibilities of BOU:

i. Onboarding billers to BBPS
ii. Ensuring compliance with due diligence requirements in respect of the onboarding of merchants prescribed in the PA Guidelines.
iii. Ensuring compliance with additional due diligence requirements that may be prescribed by NBBL for specific biller categories.
iv. Ensuring due diligence of the billers onboarded through biller aggregators.

Roles and responsibilities of COU

The BBPS Directions set out the following indicative roles and responsibilities of a COU:

i. Providing digital/physical interface to their customers, directly or through agent institutions.
ii. Ensuring customers (including customers of their agent institutions) have access to all billers onboarded on BBPS.
iii. Providing a system for raising disputes.
iv. Taking responsibility for the activities of its agent institutions, for which they have entered an agreement with the COU.

Escrow Accounts

The nodal account requirement from the erstwhile BBPS guidelines have been replaced with the opening of escrow accounts for BBPS transactions.

i. When a non-bank BBPOU collects funds from its customers or settles funds with billers onboarded by it, it functions as a payment aggregator. In line with the requirements for non-bank payment aggregators, such BBPOUs must establish an escrow account with an SCB. For the purpose of opening and maintaining this escrow account the payment system operated by the BBPOU is deemed a 'designated payment system' under the PSS Act. Additionally, any instructions on escrow accounts provided in the PA Guidelines would be applicable to the escrow maintained by a BBPOU.
ii. In the escrow account of a COU, eligible credits and debits include: (i) credits for funds collected

from customers; (ii) debits for settlement of BBPS transactions; (iii) credits or debits for failed or disputed transactions; and (iv) recovery of charges or commissions related to bill payment transactions.

iii. In the escrow account of a BOU, eligible credits and debits include: (i) debits for funds owed to the billers; (ii) credits allocated towards the settlement of BBPS transactions; (iii) credits or debits for failed or disputed transactions; and (iv) recovery of charges or commissions pertaining to bill payment transactions.

Complaint management

The erstwhile BBPS guidelines outlined a detailed grievance redressal mechanism for BBPOUs to address their customers' concerns. However, the BBPS Directions now require the establishment of the complaint management system of NBBL (NBBL CMS), which also aligns with ODR Guidelines. BBPOUs will be integrated into the 'NBBL CMS', allowing their customers to lodge complaints in accordance with this centralised platform. When addressing complaints related to failed transactions, BBPOUs must ensure that they adhere to the TAT Circular.

12. G20 declaration on DPI and AI governance

At the G20 Summit hosted by India in New Delhi from 9 – 10 September 2023, the G20 Leaders unanimously adopted the Leaders Declaration.[19] The Leaders Declaration acknowledged the significance of DPI in providing services on a large societal scale and reaffirmed the members' dedication to collaboration on global AI governance efforts.

Ahead of the G20 Summit, in August 2023 the G20 Digital Economy Ministers, along with the United Nations Development Programme and World Bank, adopted the first collectively recognised description of DPI as "a set of shared digital systems that should be secure and interoperable, that can be built on open standards and promote access to services for all, with governance and community as core components of DPI".

DPI is a core set of foundational systems that enable the use and provision of digital services across economic and social interactions. Categorisation of DPI can vary by country but generally includes digital identification, digital payments, and data exchange layers. Notable components of India's DPI for financial inclusion are:

- Aadhaar, which is a digital identification system
- UPI, which is a digital payment system
- Digilocker and account aggregator

The relevant adoptions from the Leaders Declaration are as follows:

Global adoption of DPI for sustainable development

The G20 leaders made a commitment to work towards the continued interoperability of DPI, emphasising trust-based data flow and cross-border data while respecting legal frameworks. To this end, they have recognised the following:

[19] *G20 New Delhi Leader's Declaration, 9-10 September 2023*

i. The G20 Framework for Systems of Digital Public Infrastructure,[20] a framework for the development, deployment, and governance of DPI.
ii. The Global Digital Public Infrastructure Repository,[21] a virtual repository of DPI.
iii. The Indian Presidency's proposal of the One Future Alliance (OFA),[22] an initiative to build capacity, and provide technical assistance and adequate funding support for implementing DPI in low-and middle-income countries.
iv. The G20 High-level Principles to Support Businesses in Building Safety, Security, Resilience, and Trust in the Digital Economy.[23]

Policy and regulation of crypto-assets

The G20 Leaders endorsed the Financial Stability Boards' (FSB) high-level recommendations for regulating and overseeing crypto-assets and global stablecoin activities, with a focus on ensuring effective and consistent global implementation of the recommendations to prevent regulatory arbitrage.

CBDC

The G20 Leaders acknowledged the potential macro-financial implications of the introduction and adoption of Central Bank Digital Currency (CBDC), notably on cross-border payments as well as on the international monetary and financial system. They also acknowledged the Report on CBDCs published by the Bureau of Indian Standards (BIS) and the upcoming International Monetary Fund Report on 'Potential macro-financial implications of widespread adoption of CBDCs.

Fostering responsible AI ecosystems

The G20 Leaders aim to work towards responsible, sustainable, and inclusive applications of digital technology, including the development of AI. This will include the following:

i. Leveraging AI for the common good by addressing challenges responsibly, inclusively, and in a human-centric manner while ensuring the protection of human rights, transparency, explainability, fairness, accountability, regulation, safety, appropriate human oversight, ethics, biases, privacy, and data protection.
ii. Promotion of international cooperation and facilitating discussions on international governance for AI.
iii. Advocating for innovative regulatory and governance approaches that maximise benefits while mitigating risks, and harnessing AI responsibly to achieve sustainable development goals in line with the G20 AI Principles.

---

[20]United Nations Development Programme, India's G20 Presidency, 'Accelerating the SDGs through Digital Public Infrastructure – A Compendium of the Potential of Digital Public Infrastructure'
[21]Government of India, Ministry of Electronics & Information Technology, 'Global Digital Public Infrastructure Repository'
[22]Government of India, Press Information Bureau, press release on 'Third meeting of G20 Digital Economy Working Group (DEWG) concluded on 14 June 2023', 14 June 2023
[23]G7G20 Documents Database

03

KNOW YOUR CUSTOMER FRAMEWORK

The RBI has introduced several changes to the KYC Master Directions[1] through the KYC Amendments[2] in the past year. Some of these changes were incorporated to implement various recommendations of the Financial Action Task Force (FATF)[3] ahead of the FATF's on-site inspection in November 2023. Some other changes were made to streamline and tighten KYC verification methods adopted by REs, especially for those customers who have been onboarded without meeting the RE's official, either in-person or through video-based customer identification process (V-CIP).

We have briefly summarised the key highlights of the KYC Amendments as follows:

Enhanced due diligence for non-face to face customers

Through the KYC Amendments, the RBI has directed REs to undertake Enhanced Due Diligence (EDD) measures on 'non-face-to-face customers', i.e., customers whose accounts have been opened without:

i. visiting the branch / office of the RE; or
ii. meeting the officials of the RE (either in-person or through V-CIP).

[1]Reserve Bank of India's circular titled 'Master Direction- Know Your Customer (KYC) Direction, 2016 dated 25 February 2016
[2]Amendments to the Reserve Bank of India's circular titled 'Master Direction- Know Your Customer (KYC) Direction, 2016' dated 28 April 2023, 4 May 2023 and 17 October 2023 https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT253491CD3896EC4B8F85686479E9BC39E1.PDF; https://rbidocs.rbi.org.in/rdocs/notification/PDFs/CIRCULARMDONKYC5406E44FAC85476798B09989D51F7498.PDF
[3]Financial Action Task Force's recommendations titled 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation'

Such 'non-face-to-face customers' must be categorised as 'high risk' customers and shall be subjected to 'enhanced monitoring' until their KYC verification is completed by officials of the RE on a 'face-to-face' basis (either in person or through V-CIP). The requirement for conducting KYC on a 'face-to-face' basis for regularising the risk categorisation of 'non-face-to-face customers' leads to an increase in the operational costs for conducting KYC verification.

Further, the RBI has not provided clarity on what constitutes 'enhanced monitoring'. It is unclear whether:

i. Updation of KYC documents / information of non-face-to-face customers should be done once every two years.
ii. review of risk categorisation of such customers once every six months would fulfil the requirement of conducting 'enhanced monitoring' prescribed under the KYC Master Directions.

Changes to the V-CIP framework

The validity of the secure Aadhaar XML file / Aadhaar Secure QR Code generated for V-CIP has been increased from three days to three 'working days'. Further, in rare cases where the entire V-CIP process is not completed seamlessly or in one go, REs must ensure that the video process of the V-CIP is undertaken within 'three working days' of downloading / obtaining the identification information through Central KYC Registry / Aadhaar authentication / equivalent e-document.

Reliance on CDD done by third parties

When relying on customer due diligence (CDD) done by third parties, REs must obtain such CDD records from such third parties or the Central KYC Registry immediately as opposed to the erstwhile timeline of two days.

Determination of beneficial owners

In line with Prevention of Money Laundering (Maintenance of Records) Rules PMLR,[4] through the KYC Amendments, the RBI has lowered the threshold for identifying beneficial owners of companies from ownership interest of 25% of the company's shares / capital / profit to ownership interest of 10%.

Risk categorisation

The indicative list of parameters for risk categorisation has been expanded to include geographical risk covering customers as well as transactions, type of products / services, delivery channel used, types of transaction undertaken etc. REs must keep the risk categorisation and reasons for risk categorisation of customers confidential.

Periodic updation of KYC through Aadhaar OTP based e-KYC

Through the KYC Master Directions, the RBI has permitted Aadhaar OTP based e-KYC in non-face-to -face mode to be used for periodic updation of customer KYC (i.e., once every two years for high-risk customers, once every eight years for medium risk customers and once every ten years for low-risk customers). While updating customer KYC through Aadhaar OTP based e-KYC, REs should ensure that the mobile number provided for Aadhaar authentication by the customer is the same as mentioned the mobile number mentioned in their customer profile.

---

[4] *Prevention of Money Laundering (Maintenance of Records) Rules, 2005*

04

SELF REGULATORY ORGANISATIONS

The unprecedented growth of the Fintech ecosystem in the last few years has also driven the gradual shift in RBI's approach to regulation of Fintechs from mere disclosure-based requirements to light touch and supervision, to tight regulations and finally full-fledged supervision. In various public forum discussions, the RBI has acknowledged the exponential growth of Fintechs and its support for their growth. However, at the same time, the RBI has also indicated that Fintechs need to have well-defined parameters where they evolve in the right direction, without creating any systemic risks and keeping in mind the interests of consumers. Accordingly, one of the most prominent developments in the regulatory front over the last year has been RBI's vision of setting up a self-regulatory organisation, which will be an intermediary body between the RBI and Fintechs, and the RBI and the REs.

The self regulatory organisations (SRO) are expected to act as an interface between the RBI and the Fintechs and the RBI and the REs. SROs will prescribe for the code of conduct, business ethics and certain business practices under the overarching principle-based regulations of the RBI.

We have briefly summarised some of the key details of the respective SRO frameworks as follows:

Framework for recognising SROs for Fintechs and REs

The RBI published the Draft Fintech SRO Framework[1] for comments on 15 January 2024. The Draft Fintech SRO Framework was introduced after the Draft RE Framework,[2] which was published on 21 December 2023. The draft RE Framework envisaged setting up SROs for REs. The Draft Fintech SRO Framework on the other hand, advocates for an SRO for both regulated and unregulated entities operating in the Fintech ecosystem.

The Draft Fintech SRO Framework and the Draft RE Framework recommend the creation of an SRO-FT (i.e., an SRO in the Fintech sector) and SRO-RE respectively, to provide structure, consensus, and cooperation among Fintech entities. We have briefly summarised the key aspects of the Draft Fintech SRO Framework and the Draft RE Framework as follows:

Eligibility

i. The applicant for an SRO-FT and SRO-RE must be a not-for-profit company registered in India under Section 8 of the Companies Act, 2013. SRO-FT must, in its memorandum of association, explicitly state 'operation as an SRO-FT' as a primary objective. An SRO-FT and SRO-RE should comprehensively represent the Fintech sector and the concerned sector, respectively (in terms of size, stage and activities). They should do so through voluntary memberships or they should be able to present a roadmap for achieving comprehensive representation within a reasonable timeline. Further, they should derive authority to set rules and standards for the members through their membership agreements.
ii. The RBI may invite applications for the entire Fintech sector or for specific sub-sectors in the case of SRO-FT, and for each category or class of REs in the case of SRO-RE. The number of SRO-FTs to be recognised would be considered based on the number and nature of applications received. However, the Draft RE SRO Framework does not specify such a metric for the number of SRO-REs to be recognised.
iii. A 'Letter of Recognition' will be issued to a suitable applicant(s), subject to conditions, periodic reviews, and adherence to the framework. The RBI reserves the right to deny recognition to an SRO-FT and SRO-RE, with its decision being final after providing an opportunity for the applicant to be heard.

Functions

i. SRO-FT and SRO-RE would be primarily tasked with setting standards. Such standards should be objective in nature, well-defined, customised and consultative. They would also lay down industry benchmarks, with SRO-FTs setting baseline technology standards – for transparency, disclosure, data privacy, etc. SRO-FT is also expected to prescribe standardised documents (like an agreement between a lender and

[1] Reserve Bank of India's Draft Framework titled 'Draft Framework for recognising Self-Regulatory Organisations for FinTech Sector' dated 15 January 2024
[2] Reserve Bank of India's Draft Framework titled 'Draft Framework for comments: Omnibus Framework for recognising Self-Regulatory Organisations (SROs) for Regulated Entities (REs) of the Reserve Bank of India' dated 15 January 2024

LSP that are compliant with extant statutory and regulatory requirements. Further, an SRO-FT is expected to foster professionalism through accreditation mechanisms. Both SRO-FTs and SRO-REs are required to specify the consequences for violations of agreed upon rules and misconduct.

ii. Apart from standard-setting, SRO-FTs and SRO-REs should also undertake surveillance and supervision functions, for effective monitoring and proactive interference wherever necessary. As a measure to raise awareness, they may also provide counselling on restrictive practices detrimental to sector growth.

iii. SRO-FT and SRO-RE would be involved in the promotion of statutory and regulatory understanding, compliance culture, and professionalism, as well as the dissemination of sector-specific information. They would also provide guidance and support to their members, especially smaller entities

iv. From a customer welfare perspective, the SRO-FT and SRO-RE would establish efficient, fair, and transparent grievance redressal and dispute resolution frameworks. They would also undertake activities for customer education on the various products offered in their sector within the country.

Responsibilities towards the RBI

SRO-FT and SRO-RE would act as a collective voice, addressing the larger concerns of their sector in engagements with the RBI, while being equitable and transparent to its members. They would regularly update the RBI on sector developments and notify the RBI of regulatory violations by any of its members. They would submit annual reports, periodic returns, and other information to the RBI and undertake periodic interactions with the RBI, including on its views, inputs, and suggestions. SRO-FT would also aid in policymaking and developing the taxonomy for Fintechs.

Governance and management

SRO-FT and SRO-RE must be professionally managed, governed by explicit articles of association detailing the board's functions; criteria for member admission/expulsion/suspension; and addressing conflicts of interest. The board should monitor the 'fit and proper' status of the directors of SRO-FT and SRO-RE on an ongoing basis, promptly reporting changes to the RBI. One-third of the board, of an SRO-FT, including the chairperson, should be independent from any Fintech entity. Similarly, for an SRO-RE, board members, including the chairperson, must maintain independence from entities within the relevant category or class of REs. SRO-FT and SRO-RE must possess skilled human resources and robust technical capabilities for effective sector monitoring. Additionally, the RBI may nominate/depute observers on SRO-FT's board if deemed necessary for enhanced oversight.

05

DATA PRIVACY AND FINTECHS

The Digital Personal Data Protection Act 2023 (DPDP Act)[1] places the primary obligation on 'data fiduciaries' to protect the digital personal data of individuals and implement consent artifacts, including for any outsourcing arrangements for processing. Entities that merely process such data at the behest of another entity, called 'data processors' have been excluded from the statutory compliance obligations under the DPDP Act. The DPDP Act defines 'data fiduciary' as any entity determining the means and purpose of processing personal data. Entities handling data are required to undertake this classification exercise as the first step, i.e., whether they are merely data processors or can be classified as data fiduciaries.

Fintechs are broadly categorised as entities that provide financial services through digital means or facilitate financial services through digital means. Naturally, outsourcing arrangements with Fintechs are often the lens for assessing regulatory boundaries. With extensive outsourcing of services in the Fintech ecosystem, it becomes imperative for Fintechs to assess who wears the hat of the data fiduciary or data processor under the DPDP Act. For instance, while a data analytics firm that only provides data analysis or aggregation services to a financial institution might be classified as a data processor, a loan service provider, that maintains an independent customer interface and collects

[1] *Digital Personal Data Protection Act 2023, Act No. 22 of 2023*

personal data of customers on behalf of the lending partner (but may use the same data for other purposes, such as targeted advertisements or cross-selling), may be classified as a data fiduciary. Therefore, the assessment of capacity is the first step towards compliance, and ring fencing of statutory and contractual liabilities.

Data fiduciary or significant data fiduciary

The compliance obligations are further augmented for 'significant data fiduciaries' with requirements such as the appointment of a Data Protection Officer and an independent data auditor, undertaking periodic data protection impact assessments and audits. Unlike its predecessors (the Data Protection Bill, 2019[2] and the rules framed under the Information Technology Act, 2000[3]), the DPDP Act does not provide for gradation of data into sensitive or non-sensitive for higher compliances. While it is incumbent on the Central Government to notify which entities would qualify as significant data fiduciaries, one of the determining factors for such classification includes 'sensitivity of personal data processed'. Since financial data is deemed sensitive personal data under the preceding legislation, there is the possibility of categorising Fintechs as significant data fiduciaries under the DPDP Act. It may either be based on a subjective assessment of the quality of the data being processed or a license-based classification of entities, i.e., entities having licenses from financial sector regulators.

Many hats, many masters

Fintechs are quite familiar with the regulations governing the handling of personal data. For instance, the RBI has been overseeing data management and prescribing norms, including data localisation norms,[4] data collection and storage restrictions in digital lending,[5] card data tokenisation,[6] baseline data security standards,[7] etc. This ensured that Fintechs were not caught off guard by the sophisticated consent mechanism introduced under the DPDP Act.

In anticipation of the compliance dilemma posed by the DPDP Act or sectoral norms, the DPDP Act clarifies that it should be read in addition to, rather than in derogation of, any other law. The sole caveat is that the DPDP Act would prevail in case of any conflict between the DPDP Act and any other law. A harmonious interpretation would imply that stricter compliance under the DPDP Act takes precedence over data protection stipulations in sectoral regulations and *vice versa*. This means that merely adhering to the notice – consent mechanism as envisaged under the DPDP Act would not dilute the compliances under sectoral regulations.

Exemptions and relaxations

The DPDP Act outlines specific relaxations, including exemptions from consent requirements for voluntarily provided data, as well as for certain 'legitimate purposes'. The phrase 'legitimate purposes' includes the prevention, detection, and investigation of offences, which include financial fraud and processing financial information related to loan defaults. Payment gateways, when accessing financial data like bank account or card details temporarily, may leverage the exemption for voluntarily provided data, eliminating the need for specific consent. Fintechs, depending on their data processing classifications and purposes, might find it strategic to utilise these exemptions.

---

[2]Personal Data Protection Bill 2019, Bill No. 373 of 2019
[3]Information Technology Act 2000, No. 21 of 2000
[4]Reserve Bank of India's circular titled 'Storage of Payment System Data' dated 6 April 2018
[5]Reserve Bank of India's circular titled 'Guidelines on Digital Lending' dated 2 September 2022
[6]Reserve Bank of India's circular titled 'Tokenisation – Card transactions' dated 8 January 2019
[7]Reserve Bank of India's circular titled 'Guidelines on Regulation of Payment Aggregators and Payment Gateways' dated 17 March 2020

06 REGULATING DARK PATTERNS

The Central Consumer Protection Authority has notified the Dark Patterns Guidelines[1] to prevent and regulate 'dark patterns' deployed by online platforms, advertisers, and sellers. The Dark Pattern Guidelines are issued under the Consumer Protection Act[2] and build on the Misleading Advertisements Guidelines,[3] which were also issued under the Consumer Protection Act and notified in June 2022.

What are Dark Patterns?

Dark patterns have been defined broadly in the Dark Patterns Guidelines to mean any practices or deceptive design patterns using user interfaces or user experience interactions on any platform that are designed to mislead or trick users into doing something they originally did not intend or want to do.

The practice or deceptive design should have (i) resulted in subverting or impairing consumer autonomy, decision-making or choice; and (ii) amounted to a misleading advertisement, an unfair trade practice or a violation of consumer rights.

[1] *Central Consumer Protection Authority of India, Guidelines for Prevention and Regulation of Dark Patterns, 2023*
[2] *The Consumer Protection Act 2019, No. 35 of 2019*
[3] *Central Consumer Protection Authority of India, Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022*

The Misleading Advertisements Guidelines, among other things prescribed:

The Misleading Advertisements Guidelines

01 Conditions for an advertisement to be considered valid and not misleading

02 Conditions to be met to ensure that an advertisement is not a bait advertisement

03 Prohibition on surrogate advertising

04 Duties of manufacturer, service provider, advertiser, and advertising agency

05 Guidelines for advertisements where children are targeted or children are used in advertisements

06 Guidelines to be followed when an advertisement provides that something is free or without charge

Prior to the notification of the Dark Patterns Guidelines, the Department of Consumer Affairs had been in discussions with various stakeholders to regulate dark patterns and had released draft guidelines to address dark patterns in September 2023. The Dark Patterns Guidelines, however, identify and regulate three additional dark patterns compared to those that were provided for under the draft guidelines.

The three new dark patterns are

- Trick questions
- Software as a Service (SaaS) billing
- Rogue malwares

Applicability

The Dark Patterns Guidelines are applicable to:

i. All platforms that systematically offer their goods or services in India, including digital lending platforms

ii. Advertisers

iii. Sellers

The Dark Patterns Guidelines have come into effect on 30 November 2023.

The dark patterns that are specified in the Dark Patterns Guidelines are specifically prohibited. We have set forth below an extract of these from the Dark Pattern Guidelines.

False urgency: This involves the act of dishonestly suggesting a state of urgency or scarcity to deceive a user into making an immediate purchase or taking prompt actions that result in a purchase.

Basket sneaking: This is the practice of adding extra items like products, services or charitable donations during the checkout process on a platform after a purchase, without obtaining the user's consent. It's important to note that this excludes essential fees required for order completion and taxes, which are clearly disclosed to the user at the time of purchase.

Confirm shaming: This involves employing language, videos, audio, or similar methods to instil feelings of fear, shame, ridicule or guilt in the user, with the intention of influencing them to buy a product or service from a platform. An example would be using ridicule or shame to encourage a user to contribute to charity.

Forced action: This refers to the act of compelling a user to purchase an extra product, subscribe, or register for an unrelated service or to share personal information.

Subscription trap: This involves implementing tactics that render the cancellation of a paid subscription either extremely difficult or complicated. Such practices include hiding the cancellation option for a subscription, forcing users to furnish payment details or authorising automatic debits to access a free subscription.

Interface interference: This involves implementing a design element to manipulate the user interface, emphasising particular information while concealing other pertinent details.

Bait and switch: This involves promoting a specific result tied to the user's actions but misleadingly presenting a different outcome. For example, a vendor advertises a high-quality product at an affordable price, but when the user is ready to make a purchase, the vendor marks the advertised product as unavailable and suggests a similar but more expensive alternative.

Drip pricing: This is a practice whereby prices are either not disclosed upfront or are subtly revealed during the user experience, such as charging a higher amount than the initially displayed price at the checkout.

Disguised advertisement: This refers to the strategy of disguising advertisements to appear as different types of content, such as user-generated content, news articles or deceptive ads. These ads are crafted to seamlessly blend into the overall interface, aiming to deceive users into clicking on them. The responsibility for clearly labelling such content as advertisements rests with the seller or advertiser.

Nagging: This practice entails repeatedly bothering and inconveniencing a user with various interactions, including requests, information, options or interruptions, in order to facilitate a transaction and achieve commercial benefits, unless explicitly authorised by the user.

Trick question: This involves intentionally employing unclear or ambiguous language, such as confusing wording, double negatives or similar tactics, to mislead or divert a user.

SaaS billing: This type of deceptive tactic involves exploiting positive acquisition loops within recurring subscriptions in a SaaS business model to discreetly generate and collect payments from consumers on a recurring basis. For example, the user is not notified when the free trial is converted into a paid subscription.

Rogue malware: This involves employing ransomware or scareware to deceive users into thinking their computer has a virus, with the goal of persuading them to purchase a fraudulent malware removal tool. For example, a pirated website may offer free content but introduces embedded malware when the user clicks the link.

Dark patterns are already regulated under the Consumer Protection Act. The Dark Patterns Guidelines are in addition to the general regulations and seek to provide an illustrative list of practices that will be considered dark pattern practices. The operation of dark patterns must be tested based on facts and the regulations under the Consumer Protection Act.

Next steps

Dark patterns have always been regulated by the Consumer Protection Act. However, with the introduction of Dark Patterns Guidelines specifically calling out certain dark patterns, focus is brought back to certain practices and educating consumers of their rights.

The impact of these Dark Patterns Guidelines will be substantial and will be felt more acutely for market participants in social commerce and larger e-commerce framework participants, Fintech (especially the BNPL segment), SaaS and subscription-based service providers.

It would be trite for the market participants to quickly put in place processes to ensure that they are not caught wrong-footed. While there is no general formula to set the table in order and each industry and business has different considerations, some key practices that can be considered across all market participants are set forth below:

i. **Review existing practices:** Market participants should review their existing user interface, user experience interactions, and consumer facing practices to ensure that none of them could be construed as a dark pattern. These should be reviewed on a periodic basis.
ii. **Training:** Market participants should train staff and other ecosystem participants on the need to adhere to good practices and stay away from any practice that can be construed as a dark pattern.
iii. **Consumer focused flows:** Going forward, market participants should ensure best practices in educating consumers of their rights, making proper disclosures, and making offers and accepting consents fairly.
iv. **Grievance redressal:** Consumers should be provided with the ability to reach out to market participants to communicate grievances. Once grievances are received, market participants should act promptly and keep consumers informed of the resolution process.
v. **Other considerations:** Terms and conditions and other consumer facing agreements should be reviewed to build safeguards for instances where third-party acts affect the service or products provided by platforms.

The regulatory framework introduced by the Dark Patterns Guidelines is expected to reinforce an increased sense of accountability among market participants, specifically sellers and advertisers thereby reshaping the landscape of consumer commerce, specifically in the digital space.

07

IT FRAMEWORK

Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices[1]

The RBI published the IT Master Directions on 7 November 2023. The IT Master Directions updates, consolidates and harmonises the separate instructions issued by the RBI on aspects such as IT governance and controls, business continuity, information systems audits, etc. To this effect, the IT Master Directions repeals and substitutes several erstwhile circulars on the said matters, including the NBFC IT Directions[2] (which continue to apply to the NBFC – Base Layer). We have briefly analysed some of the key provisions of the IT Master Directions below:

Applicability

The IT Master Directions are applicable to all SCBs, small finance banks, payments banks, NBFCs (except NBFC-Base Layer), Credit Information Companies (CICs), and All India Financial Institution (AIFIs). Local area banks and NBFCs – Core Investment Companies are specifically excluded from the applicability of the IT Master Directions. For foreign banks operating in India through branch mode, the controlling office / head office having oversight over such branch operations in India is vested with the responsibilities imposed on the Board of Directors under the IT Master Directions. Further, the RBI has adopted a 'comply-or-explain' approach towards the

[1]*Reserve Bank of India's circular titled 'Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices' dated 7 November 2023*
[2]*Reserve Bank of India's circular titled 'Master Direction - Information Technology Framework for the NBFC Sector' dated 8 June 2017*

implementation of the IT Master Directions for such foreign banks. The IT Master Directions come into force from 1 April 2024.

Formulation of IT governance framework

REs are now required to put in place an IT governance framework, that clearly specifies (i) the governance structure and processes aligned with the business/strategic objectives of the RE; (ii) the specific roles and responsibilities of the board and other committees; and (iii) oversight mechanisms for accountability and mitigation of risks. The IT Master Directions also mandate periodic assessments of IT-related risks.

Key stakeholders in governance structure

REs are now required to overhaul their IT governance structure and segregate them into two independent verticals: (i) IT infrastructure; and (ii) IT security. Both IT infrastructure and IT security are expected to be supervised by the Information Technology Strategy Committee (ITSC) of the Board of Directors.

Board of Directors and ITSC

The Board of Directors is entrusted with the responsibility for the formulation and annual review of all IT infrastructure and IT security related policies and the constitution of the ITSC. ITSC is a board-level committee comprising a minimum of three directors and members who are technically competent. ITSC reports to the Board of Directors. The ITSC is also required to have a chairperson who is an independent director and has substantial IT expertise in managing / guiding information technology initiatives. Substantial IT expertise has been defined as a minimum of seven years of experience in managing information systems and/or leading / guiding technology / cybersecurity initiatives / projects and having an understanding of business processes at a broader level and the impact of IT on such processes. It is entrusted with the responsibility of ensuring that the RE has an effective IT strategic planning process, guiding in the preparation of the IT governance and information security governance structure, processes for assessing and managing IT and cybersecurity risks, adequacy of budgetary allocation for IT functions, and reviewing annually the adequacy of the business continuity planning and disaster management of the RE.

The ITSC is, in turn, responsible for the implementation and review of strategies for IT infrastructure and IT security. The brief governance structure for IT infrastructure and IT security at the management level is set out below:

IT infrastructure

i. **Senior Management:** There is no specific definition of senior management, and senior members of the management, like Chief Technology Officers, Chief Executive Officers, Chief Operating Officers, departmental heads, would constitute senior management. They are entrusted with the responsibility of implementing the IT strategies and reporting to the ITSC.

ii. **IT Steering Committee:** The ITSC is also required to have an IT Steering Committee comprising senior management. The IT Steering Committee is entrusted with the responsibility of assisting the ITSC in its functions, overseeing the processes for business continuity and disaster recovery, and implementing the IT architecture, and ensuring that it meets statutory and regulatory compliance.

iii. **Head of IT Functions:** The RE is also required to appoint an official at a sufficiently senior level, who is technically competent and experienced in IT related aspects. The main role of the head of IT Functions is to ensure that the execution of IT projects / initiatives is aligned with IT policy /

strategy, effective organisational structure to support IT functions and put in place an effective disaster recovery setup and business continuity strategy.

IT security

i. **Information Security Committee (ISC):** The ISC is formed under the oversight of the ITSC. Its responsibilities are primarily oriented towards risk mitigation and include formulating information / cybersecurity policies and the implementation of policies and processes to ensure that identified risks are managed within the RE's risk appetite, approving and monitoring information security projects, reviewing cyber incidents, information security audit observations, monitoring and mitigation and updating ITSC and the chief executive officer of its activities periodically.

ii. **Chief Information Security Officer (CISO):** CISO is a senior level executive, preferably in the rank of general manager or an equivalent position. It is not to have a direct reporting relationship with the head of IT Functions and not to be given business targets. They are also a permanent invitee to the ITSC and IT Steering Committee. Their responsibilities mainly relate to cybersecurity, and include driving the cybersecurity strategy and ensuring compliance with cybersecurity related regulations, enforcing policies for the protection of information assets, ensuring the effective functioning of security solutions deployed, coordinating internally and with external agencies on cybersecurity issues, managing and monitoring Security Operations Centre SOC, placing a review of cybersecurity risks arrangements / preparedness of the RE on a quarterly basis.

Key obligations

Along with the governance structure, the IT Master Directions also provide for the following key obligations of REs:

i. Setting up a robust IT Service management framework so as to ensure the operational resilience of their IT environment and the use of updated hardware and software.

ii. Putting in place a broad framework for regulation of third-party arrangements that do not fall within the scope of the IT Outsourcing Directions[3] and is centred on vendor risk assessment and controls, which incorporates factors, concentration risk, conflict of interests, compliance with data protection regulations and standards and supply chain risks.

iii. Obtaining the source codes of critical applications from their vendors, and where they cannot be obtained, ensuring that they enter into appropriate arrangements, which may include source code escrow arrangements, to mitigate the risk of default on the part of the vendor.

iv. Setting up data related regulations and controls involving migration, audit trail, cryptographic controls, cyber incident response and recovery management.

v. Setting up appropriate physical and environmental controls in their data centre and disaster recovery sites, including necessary e-surveillance mechanisms. Further, the data centre and disaster recovery site is required to be geographically well separated to avoid both sites being affected by similar geographical threats.

---

[3]*Reserve Bank of India's circular titled 'Master Direction on Outsourcing of Information Technology Services' dated 10 April 2023*

vi. Setting up physical and environmental controls, access control, vulnerability assessment and penetration testing.
vii. Ensuring that audit committee of the RE conducts an audit of the RE's Information Systems, addressing critical issues and offering guidance to the RE's management based on their findings.

The IT Master Directions provide for a comprehensive and consolidated framework on the governance of IT, information systems, business continuity and disaster recovery. In line with the recent trends, RBI has harmonised the separate frameworks applicable to banks, NBFCs and other financial services REs via the IT Master Directions. While the IT Master Direction's ambit is comprehensive, there is still a degree of ambiguity on whether certain requirements are mandatory or recommendatory in nature.

Further, given the overhaul in the governance structure, while most banks and NBFCs would have many of the stipulated controls already in place owing to the extant circulars applicable to them, they would have to align their organisational structure and appoint personnel with appropriate skills and expertise, as required under the IT Master Directions. NBFCs would now be required to implement stringent technology-related controls, akin to the standards in place for banks. While this would inevitably drive-up compliance costs, such measures would go a long way in strengthening cybersecurity and information security at an organisational level.

Other REs, such as small finance banks and CICs, which are currently sparsely regulated in this space, would have to considerably reevaluate their present technological, as well as organisational structure and processes. They would also be required to devise compliant policies in line with the new requirements.

Fintechs, technology service providers, cloud service providers and other enablers, who are otherwise unregulated by RBI, would also have to rejig some of their present processes in order to support and enable REs to comply with the new compliance obligations. Appropriate amendments in contractual arrangements between REs and such service providers and partners may also be required for REs to ensure secondary compliance requirements. For instance, the Digital Lending Guidelines place the onus on the REs to ensure that the LSPs engaged by them also comply with the various technological standards/requirements on cybersecurity as stipulated by the RBI for undertaking digital lending, which now includes the IT Master Directions.

08 SECURITIES AND INVESTMENT PLATFORMS

The RBI has played an instrumental role in the development of India's Fintech industry. However, the fintech landscape is dynamic with ever increasing intersection of the activities of Fintech platforms with the securities market. In this light, the role of the Securities and Exchange Board of India (SEBI) and other regulators in the financial markets space becomes particularly significant. Some of the key areas that have caught the attention of SEBI have ranged from social media personalities influencing financial decisions and the regulatory oversight there, fractional ownership platforms aiming to govern Fintech offerings related to fractional ownership in commercial real estate, and asset tokenisation representing futuristic opportunity by transforming real-world asset ownership into digital tokens through blockchain technology. We have briefly summarised some of the key highlights below:

1. SEBI'S regulatory oversight over 'Finfluencers'

The rise of social media marketing has led to the emergence of 'finfluencers' or content creators, who by virtue of their reach on various social media platforms, such as Instagram, X (formerly known as Twitter), Facebook and Youtube, are in a reasonable position to influence the financial decisions including investment in financial products through paid promotions or recommendations otherwise. However, it has been observed that the finfluencer content suffers from lack of transparency, potential conflicts of interest and lack of regulatory oversight. Finfluencers may offer biased or misleading recommendations to their audience which are rooted in their own gains rather than that of the consumers. The content also often lacks nuances required for informed financial decisions under the guise of easily digestible content. SEBI recognising the threat of unregulated finfluencers, has recently taken several steps to put a check on such activities.

SEBI's Consultation Paper

On 25 August 2023, SEBI released the SEBI Consultation Paper[1], aimed at limiting the association of SEBI registered entities and REs with unregistered entities like finfluencers. The SEBI Consultation Paper recognises that finfluencers are operating either as regulated entities registered with relevant regulators, such as, SEBI, RBI, Pension Fund Regulatory and Development Authority, or Insurance Regulatory and Development Authority, or operating without any registrations, licenses and permits (i.e., unregulated entities).

The SEBI Consultation Paper proposes to bring about the following regulatory changes:

Prohibitions on SEBI registered entities and their agents

i. No monetary or non-monetary relationship for any promotion or advertisement of their services/products, with any unregistered finfluencer.
ii. No sharing of any confidential information of their clients with any unregistered finfluencer.
iii. No payment of a trailing commission as referral fee to unregistered finfluencers. For instance, for a mutual fund product purchased by a consumer in the influence of a finfluencer, through his / her referral link, no referral fee may be made payable to the finfluencer as commission for the consumer holding the mutual fund product.

Requirements for registered finfluencers

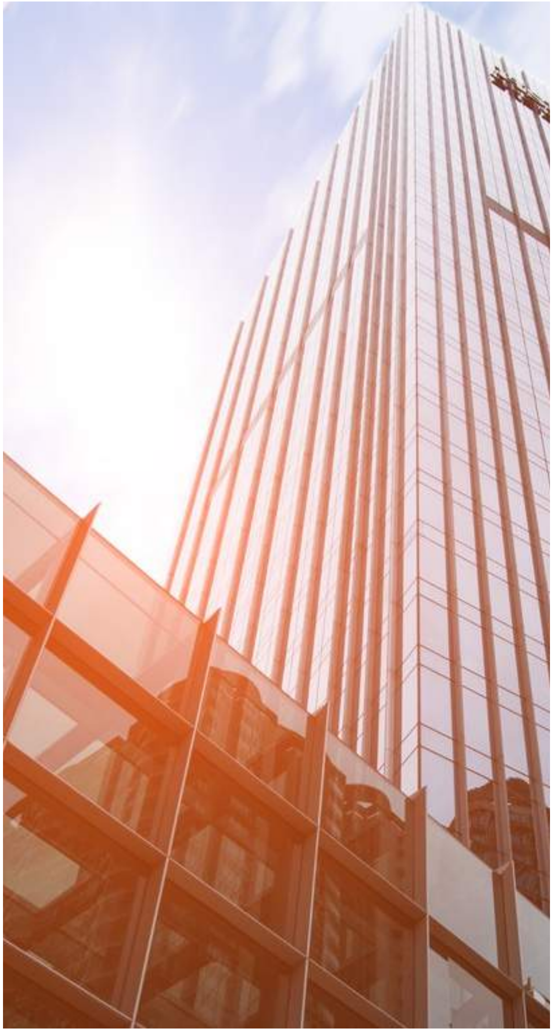
i. Finfluencers registered with SEBI or stock exchanges or Association of Mutual Funds in India, to be required to display registration number, contact details, investor grievance redressal helpline, along with appropriate disclosure and disclaimer on all their posts.
ii. Registered finfluencers to comply with the code of conduct under their relevant regulations and the advertisement guidelines issued by SEBI, stock exchanges & SEBI recognised supervisory body.

SEBI's regulatory intervention

While the proposed regulatory changes under the SEBI Consultation Paper have not been formalised yet, SEBI continues to take active steps to keep unregulated finfluencer activities in check. In one of its earliest actions against finfluencers, SEBI on 25 May 2023 (Settlement Order in the matter of Mansun Consultancy Pvt. Ltd.[2]), penalised popular financial influencer PR Sundar for violating investment adviser norms by providing advisory services without the necessary registration from the regulator on various platforms, including chat platforms like Telegram.

[1] *Securities Exchange Board of India's consultation paper titled 'Association of SEBI Registered Intermediaries / Regulated Entities with Unregistered Entities (including Finfluencers)' dated 25 August 2023*
[2] *Securities Exchange Board of India's settlement order in the matter of 'Mansun Consultancy Private Limited' dated 25 May 2023*

More recently, SEBI in its interim order dated 25 October 2023[3] cracked down on a certain finfluencer without being registered with SEBI as an investor advisor meting out 'investment advice' under the garb of educational courses on the securities market. SEBI found the finfluencer disseminating trading strategies on YouTube that promised quick, consistent and assured returns. Additionally, the finfluencer was found conducting physical workshops on securities market and circulating messaged on private chat groups with investors who subscribed to his educational courses, offering buy/sell/hold recommendations. SEBI read the promising prospects of profit on adopting certain investment strategy to fall within the scope of 'investment advice' which necessitates necessary registrations to be undertaken. Given the increased scrutiny of financial influencers, there is an urgent requirement for regulations governing this sector. It is anticipated that SEBI will promptly introduce pertinent regulations to offer essential clarity on the matter.



2. Fractional ownership platform

In the last two years, several web-based platforms offering fractional ownership of real estate assets have emerged. These 'fractional ownership platforms' (FOPs) generally incorporate special purpose vehicles (SPVs) which own underlying real estate projects. Through the FOP, retail investors are provided with an opportunity to invest in the shares / capital of the SPVs and thereby, own a fractional portion of the underlying real estate projects (*pro rata* to their investment in the SPVs). Return on such investments is primarily generated through rental income and proceeds from sale of real estate projects. However, it has been observed that FOPs often operate in an ambiguous and opaque manner, and that their operations are not subject to independent review and oversight.

SEBI FOP Consultation Paper

Recognising the threat of unregulated FOPs, the SEBI released the SEBI FOP Consultation Paper,[4] aimed at bringing FOPs under the direct regulatory supervision of SEBI. The SEBI FOP Consultation Paper proposes to bring about the following regulatory changes:

i. Registration requirements for FOPs

a. Any person or entity (including FOPs) which facilitate or have facilitated fractional investment in real estate by any structure whatsoever shall obtain registration as a 'MSM REIT' (Micro, Small and Medium Real Estate Investment Trusts) under the REIT Regulations.[5]
b. Such entities must fulfil eligibility criteria as prescribed by SEBI from time to time and obtain registration, failing which, they shall be required to wind up their operations after giving existing investors the ability to exit.

[3] Securities Exchange Board of India' interim order in the matter of 'Unregistered Investment Advisory Activities by Mohammad Nasiruddin Ansari / Baap of Chart' dated 25 October 2023
[4] Securities Exchange Board of India's consultation paper titled 'Regulatory Framework for Micro, Small and Medium REITs (MSM) REITs' dated 12 May 2023
[5] Securities Exchange Board of India's circular titled 'SEBI (Real Estate Investment Trusts) Regulations, 2014' dated 26 September 2014

ii. Structure of MSM REITs

a. MSM REITs are required to be set up as a trust under the Indian Trusts Act, 1882 and must have the ability to establish separate and distinct scheme(s) for owning of real estate assets through wholly owned SPVs incorporated as companies under the Companies Act 2013.
b. The MSM REIT scheme must have full control and must hold 100% of the equity share capital of all the SPVs. The SPVs in turn must have full control and must hold 100% ownership in all the underlying real estate projects.

iii. Key appointments

a. All MSM REITs must appoint a trustee, a sponsor and an investment manager.
b. The sponsor must have at least five years of experience in the real estate business as a developer or fund manager; and a net-worth of INR 20,00,00,000 (~USD 2,400,000), out of which INR 10,00,00,000 crore (~USD 1,200,000) must be in the form of liquid net worth (i.e., cash, money market instruments, Government Securities, Treasury Bills).
c. The Investment Manager must have at least five years of experience in development of real estate or management of real estate (i.e., providing fund management / property management / advisory services). The manager must also have a net-worth of INR 10,00,00,000 (~USD 1,200,000) which must be in the form of liquid net worth (i.e., cash, money market instruments, Government Securities, Treasury Bills).

SEBI Press Release

Through the SEBI FOP Press Release,[6] the SEBI Board communicated that it had approved amendments to the Real Estate Investment Trusts (REIT) Regulations to give effect to a regulatory framework for governing the activities of entities facilitating fractional investment in real estate. While the SEBI Press Release does not provide complete details of the amendments which have been approved, there is one clear deviation from the SEBI FOP Consultation Paper: while the SEBI FOP Consultation Paper proposed a minimum asset value of INR 25,00,00,000 (~USD 3,000,000), the SEBI Press Release states that the minimum asset value shall be INR 50,00,00,000 (~USD 6,000,000).

The increased threshold for asset value is also reflected in the different terminologies used in the SEBI FOP Consultation Paper and the SEBI Press Release: in the former, entities facilitating fractional investment in real estate were proposed to be regulated as 'Micro, Small & Medium REITs' whereas in the latter, it is stated that such entities will be regulated as 'Small & Medium REITs'.

Even though the SEBI Board has approved amendments to the REIT Regulations to regulate entities facilitating fractional investment in real estate, the amendments themselves are yet to be notified.

[6] *Securities Exchange Board of India's press release titled 'SEBI Board Meeting' dated 25 November 2023*

GLOSSARY

ACH	Automated Clearing House
AI	Artificial intelligence
AIFI	All India Financial Institution
AD Banks	Authorised Dealer Category I banks
AFA	Additional Factor Authentication
Agent Institutions	An entity, certified by NBBL, which provides customer interface (physical / digital) for bill payments
BBPS	Bharat Bill Payment System
BBPS Directions	Reserve Bank of India (Bharat Bill Payment System) Directions, 2024
BBPCU	Bharat Bill Pay Central Unit
BBPOU	Bharat Bill Payment Operating Unit
Biller Aggregator	An entity which aggregates billers for the purpose of enabling them to connect to a BOU
BIS	Bank for International Settlements
BOU	Biller Operating Unit
BPSP	Business Payment Solution Provider
CBDC	Central Bank Digital Currency
CCPA	Central Consumer Protection Authority
CDD	Customer Due Diligence
CIC	Credit Information Companies
CISO	Chief Information Security Officer
Consumer Loan Circular	RBI Circular on Regulatory Measures Towards Consumer Credit and Bank Credit to NBFCs dated 16 November 2023
COU	Customer Operating Unit
Dark Pattern Guidelines	'Guidelines for Prevention and Regulation of Dark Patterns' issued by the CCPA on 30 November 2023
Digital Lending Guidelines	RBI Guidelines on Digital Lending dated 2 September 2022
DLG	Default Loss Guarantee
DLG Guidelines	RBI Guidelines on Default Loss Guarantee (DLG) in Digital Lending dated 8 June 2023
DLG Provider	An unregulated Fintech company or RE that guarantees to compensate the RE Lender for a loss due to default up to a certain specified percentage of the loan portfolio of the RE.
DPDP Act	Digital Personal Data Protection Act, 2023
DPI	Digital Public Infrastructure
Draft Fintech SRO Framework	RBI Draft Framework for Recognizing Self-Regulatory Organisations (SRO) for FinTech Sector dated 15 January 2024
Draft RE SRO Framework	RBI Draft Framework for Omnibus Framework for recognising Self Regulatory Organisations for Regulated Entities dated 21 December 2023.
ECA	Export Collection Account
EDD	Enhanced Due Diligence
EDPMS	Export Data Processing and Monitoring System
e-KYC	Electronic know-your-customer
e-Mandate Circular	NPCI Circular on E-Mandate Simplification and Harmonization of the Limit of all Variants of Mandates dated 21 July 2023
EMI	Equated Monthly Installments
FAQ	Frequently Asked Questions
FATF	Financial Action Task Force
FEMA	Foreign Exchange Management Act 1999
Fintech	Financial Technology
FIU-IND	Financial Intelligence Unit – India
FLDG	First Loss Default Guarantee
FOP	Fractional Ownership Platform
FSB	Financial Stability Board
G20 AI Principles	The principles for responsible stewardship of trustworthy AI adopted by the G20

G20 Leaders	The finance ministers and central bank governors of participant nations of the G20 that lead the finance track of every G20 Summit
G20 Summit	The G20 Summit hosted by India in New Delhi from 9 – 10 September 2023
GIFT City	Gujarat International Finance Tec-City
HFC	Housing Finance Companies
ICA	Import Collection Account
IDPMS	Import Data Processing and Monitoring System
IFSC	International Financial Services Centre
IFSCA	International Financial Services Centre Authority
IMPS	Immediate Payment Service, a payment system managed by the NPCI
IT	Information Technology
IT Master Directions	Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023
IT Outsourcing Directions	Reserve Bank of India (Outsourcing of IT Services) Directions, 2023
ITSC	IT Strategy Committee
ISC	Information Security Committee
INR	Indian Rupee
KYC	Know-your-customer
KYC Amendments	Amendments made to the KYC Master Directions over the course of 2023
KYC Master Directions	Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016
Leaders Declaration	The New Delhi Leaders Declaration adopted by the G20 Leaders
LSP	Lending Service Provider
MSME	Micro, Small & Medium Enterprises
MSM REIT	Micro, Small and Medium Real Estate Investment Trusts
NACH	National Automatic Clearing House
NBBL	NPCI Bharat Bill Pay Limited
NBBL CMS	The complaint management system established by NBBL
NBFC	Non – Banking Financial Company
NBFC IT Directions	Information Technology Framework for the NBFC Sector – Directions, 2017
NEFT	National Electronic Funds Transfer, an electronic funds transfer system maintained by the RBI
NFC	Near Field Communication
NPA	Non – Performing Assets
NPCI	National Payments Corporation of India
ODR	Online Dispute Resolution
ODR Guidelines	RBI Directive on Online Dispute Resolution (ODR) System for Digital Payments dated 6 August 2020
OPGSP	Online Payment Gateway Service Provider
OTP	One time password
PA	Payment Aggregator
PA Guidelines	RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways dated 17 March 2020
PA-CB Guidelines	RBI Circular on Regulation of Payment Aggregator – Cross Border (PA – Cross Border) dated 31 October 2023
PA – CB	Payment Aggregator – Cross Border
PAN	Permanent Account Number
PayPal Judgement	PayPal Payments v Financial Intelligence Unit India; 2023 SCC OnLine Del 4336
Penal Interest Circular	RBI Circular on Fair Lending Practice – Penal Charges in Loan Accounts dated 18 August 2023
Penalty Circular	NPCI Circular on penalty for high percentage of ACH debit returns dated 18 August 2023
PMLA	Prevention of Money Laundering Act 2002
PMLR	Prevention of Money Laundering (Maintenance of Records) Rules, 2005
PPIs	Prepaid Payment Instruments
PPI Master Directions	Reserve Bank of India Master Directions on Prepaid Payment Instruments, 2021
PSP Banks	Payment system providers that are banks
PSS Act	Payment and Settlement Systems Act, 2007
PSO	Payment System Operator
QR	Quick Response

RBI	Reserve Bank of India
RE	Regulated Entity
RE Lender	RE that acts as the lender in an DLG arrangement
REIT	Real Estate Investment Trusts
REIT Regulations	Securities and Exchange Board of India (Real Estate Investment Trusts) Regulations, 2014
Report on CBDCs	Report submitted by BIS dated 11 July 2023 to the G20 Finance Ministers and Central Bank Governors titled 'Lessons learnt on CBDCs'
RTGS	Real-time gross settlement, a payment system maintained by the RBI
SCB	Scheduled Commercial Bank
SEBI	Securities and Exchange Board of India
SEBI Consultation Paper	SEBI's consultation paper on Association of SEBI Registered Intermediaries / Regulated Entities with Unregistered Entities (including Finfluencers) dated 25 August 2023
SEBI FOP Consultation Paper	SEBI consultation paper titled 'Regulatory Framework for Micro, Small and Medium REITs (MSM REITs)' dated 12 May 2023
SEBI FOP Press Release	SEBI's press release titled 'SEBI Board Meeting' dated 25 November 2023
Secured Assets	Original movable property or immovable property documents and the charge thereon
Secured Assets Directions	RBI Circular on Responsible Lending Conduct – Release of Movable / Immovable Property Documents on Repayment / Settlement of Personal Loans dated 13 September 2023
SOC	Security Operations Centre
SPV	Special Purpose Vehicle
SRO	Self-Regulatory Organisations
SRO-FT	SRO for the Fintech sector
SRO-RE	SRO for Regulated Entities
TAT	Turn Around Time
TAT Circular	RBI Circular on Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems dated 20 September 2019
TPAPs	Third Party Application Providers
TSPs	Technology Service Providers
UK	United Kingdom
UPI	Unified Payments Interface
UPI Credit Lines Circular	RBI Circular on Operation of Pre-Sanctioned Credit Lines at Banks through Unified Payments Interface (UPI) dated 4 September 2023
USD	United States Dollar
V-CIP	Video-based Customer Identification Process

Industry Outlook

"While there has been a great buzz about Fintech in the last decade, we have only seen the tip of the iceberg of disruption in the financial sector. With outsourcing of technology in the financial sector continuing to gain momentum, specialised service providers are set to further improve customer experience and access to financial services, as well as reducing costs and efforts for financial institutions. With regulations around financial services and IT services outsourcing consolidating lately, compliance becomes key, not only for the regulated entities, but also for the aspirational service providers eyeing to revolutionise and democratise the financial services in India."

Ramgopal Subramani, Chief Strategy Officer, Perfios Software Solutions

---

"Over the last few years, the Fintech and Fintech infrastructure has seen unprecedented growth and emergence of many good companies, which are now moving from early / mid stages to growth / late stages. As the competition and stakes increase in this segment, and with the emergence of new technologies and models, the incumbents will need to work extra hard to continue growth trajectories and it'll be equally difficult for the new entrants to break through to the already earned trust of customers by the incumbents. I expect the next year to be exciting and full of ebbs and flows."

Mehekka Oberoi, Fund Manager-Fintech, IIFL Group

"With abundant opportunities, but often limited resources, innovation becomes the cornerstone of disruption in the fintech sector in India. From AI-powered analytics to API-based solutions, technology is redefining the financial landscape, enhancing efficiency, and fostering financial inclusion. Such intersection of the conventional financial industry and new-age tech holds the key to unlocking new possibilities and reshaping traditional banking. Embracing these advancements is not just a choice but a necessity for players aiming to thrive in the dynamic fintech ecosystem of India. India seems poised to pioneer advancements in fintech in the coming decade, as it did in the last."

Nikhil Kumar, Co-founder, Setu

"What makes India's fintech sector standout is a defining characteristic: agility with which its businesses pivot product offerings to align with the regulatory needs. The sector continues to grow, mature and display great resilience in the process."

Vardaan Ahluwalia, Head – Legal, Premji Invest

“The industry envisions the digital lending sector evolving with the regulator’s intent to provide legitimacy through comprehensive guidelines and regulatory frameworks. Having closely observed the sector, I see good opportunity of growth in the digital lending sector, and also the importance of heightened data compliances and regulatory safeguards. This dual approach fosters innovation while safeguarding consumer interests, creating a dynamic landscape for sustainable growth and enhanced customer experiences in the digital lending realm.”

Ashwani Tyagi, General Counsel, super.money

“NBFCs have shown great agility in adapting with shifting consumer needs and preferences and regulatory changes in the recent past. NBFCs have leveraged technology to streamline retail loans, vehicle loans, gold loans and several such product offerings, which cater to a wide segment and strata of consumers. However, rapid expansion was also marked by checks and balances, including the RBI prompting us to wear our thinking hats back on with its emphasis on risk weight on unsecured loans. The intent is clearly towards responsible lending practices. We anticipate continued momentum in digital transformation and financial inclusion while maintaining compliance checks and customer trust.”

Vikas Arora, Chief Compliance Officer, TVS Credit

“We are at a pivotal moment where MSME credit is poised to take center stage. OCEN’s groundbreaking framework not only revolutionizes short-term lending profitability by reducing costs but also establishes open standards in the lending value chain. With its robust dispute management system and tech-legal approach, OCEN aids regulation, ensuring transparency and efficiency. By establishing rails for the MSME lending ecosystem to thrive and scale multifold, OCEN is shaping the future of lending in India.”

Sagar Parikh, OCEN lead, iSPIRT

“Digital lending in India has seen tremendous growth in the last decade or so. While the industry has been pioneering with creative solutions, the regulator has also been doubling down on regulatory compliances to check systemic risks in the economy. The last year was in particular pivotal for digital lending, with the regulator legitimising FLDG and laying down strict norms on IT outsourcing. Such regulations highlight heightened importance of sustainable collaboration between regulated and unregulated entities, by determining responsibilities and liabilities upfront. Collaborative efforts between regulators, regulated financial institutions, and fintech players will be pivotal in determining the future for the digital lending segment in India.”

Ashish Gupta, MD & Business Head, MSME & Education Digital Loans, JM Financial Products

---

Contact us

Khaitan & Co

Sanjay Khan Nagra
Partner
sanjay.khan@khaitanco.com

Smita Jha
Partner
smita.jha@khaitanco.com

Prashanth Ramdas
Partner
prashanth.ramdas@khaitanco.com

Digital Lenders Association of India

For queries, please write to us at
contact@dlai.in

Contributors

Ganesh Prasad | Supratim Chakraborty | B N Vivek | Sumantara Bose
Pritish Mishra | Diksha Singh | Nikita Nagori | Riddhiman Sarkar | Ishani Sahai
Shramana Dwibedi | Rashi Rawat | Apoorva Singh | Jino Mathews Raju
Viti Bansal | Navya Saxena

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1,000 legal professionals, including 220 Partners and Counsel, and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

The Fintech practice of the firm envisions to emulate the firm's ambition of being the trusted advisor to its clients on all aspects of Fintech offerings, including regulatory, compliances, product advisory, disputes, investments, partnerships, and licensing / approvals.

To know more about us, please visit www.khaitanco.com

About Digital Lenders Association of India

Digital Lenders Association of India (DLAI) was formed in November 2016 with the objective of bringing together digital lenders and their associated players under one roof to form an association that would help the ecosystem grow and flourish. Its primary objective is to unite digital lenders (MSME and consumer), marketplace platforms, and industry members to create a platform for sharing best practices, conduct research on innovative business models, and work with regulators, industry experts, and other government bodies to set broad contours on policy matters beneficial to the entire digital credit industry.

To know more about us, please visit www.dlai.in