Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI SILICON VALLEY BENGALURU SINGAPORE NEW DELHI NEW YORK GIFT CITY

Research

Fintech

Legal, Regulatory and Tax Considerations – Compendium

January 2025

Research

Fintech

Legal, Regulatory and Tax Considerations – Compendium

January 2025

DMS Code: 113629.1

About NDA's FinTech Practice

We have significant experience in the financial services over technology (FinTech) industry since its beginning in India and advise several leading players in the industry as well as industry associations. We have developed expertise and carved a niche in this area through comprehensive research, in-depth understanding and monitoring of the sector. We were the lead firm representing the Internet and Mobile Association of India in its successful Supreme Court challenge to the Reserve Bank of India restriction on virtual currencies, resulting in a first-of-its-kind landmark judgment allowing banks and other regulated entities to facilitate trading in cryptoassets, hence opening up the ecosystem in India. We advise regulated entities in the FinTech industry such as payment aggregators, prepaid payment instrument issuers, other payment system operators, banking partners, cross-border service facilitators, as well other stakeholder entities such as merchants and technology providers on a regular basis. We provide varied services ranging across advisory, disputes and litigation, regulatory and policy initiatives, documentation and transactions assistance. We have closely worked with financial regulators such the RBI and SEBI on obtaining regulatory licenses and setting up regulated business operations, advised our clients on regulatory issues and compliance requirements considering the global outlook of their business, as well as guided them to structure their business and product to the most optimum level while navigating applicable legal compliances effectively. We advise a diverse clientele comprising global MNCs, investment funds, unicorns, startups, intermediaries and service providers with market leading products in industries ranging from the banking, digital media, e-commerce and gaming sectors.

Our experience not only helps us in executing cutting edge matters but also assists in making policy recommendations to the Government of India. We have been involved with industry representative associations such as the Blockchain Association Singapore (BAS), NASSCOM (National Association for Software and Services Companies), DSCI (Data Security Council of India), USIBC (US-India Business Council), IAMAI (Internet and Mobile Association of India) and FICCI (Federation of Indian Chambers of Commerce & Industry) amongst others for several years in terms of policy reforms for the IT sector since the early 2000s. We regularly provide feedback on various RBI regulations, provide our recommendations on various draft laws and consultation papers released by different Government ministries, attend open house discussions held by different Government ministries and engaging in dialogue with the regulators seeking clarifications on various grey areas under the law. For instance, we have made representations to the RBI on cyber security framework in the banking sector, alternative solutions to counter restrictions on card data storage requirements such as card-on-file tokenization, drafted self-regulatory code of conduct for the blockchain industry association and drafted an independent policy paper submitted to the Government of India suggesting ways towards the regulation of crypto-assets in India, which we were invited by the Ministry of Finance to present in person.

FT INNOVATIVE LAWYERS 2019
FINANCIAL TIMES
ASIA-PACIFIC WINNER

Ranked as the 'Most Innovative Indian Law Firm' in the prestigious FT Innovative Lawyers Asia Pacific Awards for multiple years. Also ranked amongst the 'Most Innovative Asia Pacific Law Firm' in these elite Financial Times Innovation rankings.

Chambers AND PARTNERS

IFLR1000

The LEGAL 500

BENCHMARK LITIGATION

asialaw

WWL

ASIAN LEGAL BUSINESS

INDIA BUSINESS LAW JOURNAL

INDIA BUSINESS LAW JOURNAL THE A LIST 2023 2024 LAW ASIA

INDIA BUSINESS LAW JOURNAL DEALMAKER 2023 LAW ASIA

Mergermarket An Acuris company

ITR WORLD TAX

iel ELITE

BUSINESS TODAY

THE NATIONAL LAW REVIEW

equalFi

ILA IDEX LEGAL AWARDS

LEGAL ERA BY THE PEOPLE. FOR THE PEOPLE. OF THE PEOPLE

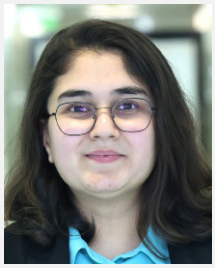
LawWiser .com

Disclaimer

Contact

For any help or assistance please email us on **concierge@nishithdesai.com**
or visit us at **www.nishithdesai.com**.

Compiled by



Palak Kapoor
palak.kapoor@nishithdesai.com

Aaron Kamath
aaron.kamath@nishithdesai.com

Contents

Digital Payments

November 7, 2024

A. India's Data Localisation for Payment Systems: Origins, evolution, and the road ahead

Click the above logo to visit the published article

According to the Reserve Bank of India's (RBI) Currency and Finance report for 2023-24, the average cost of data breaches in India reached $2.18 million in 2023. This is a 23% uptick from the previous year and 15% across the last three years.[1] This worrying trend in the recent times has prompted the RBI to take stricter mechanisms to prevent data breaches especially with respect to sensitive financial data. One of the most sensitive forms of such financial data is payments data. Since 2018, the RBI has introduced a series of regulations aimed at mandating the localisation of payments data to ensure its security. These regulations cover areas such as the storage of payments data, the conduct of payment aggregators, and the tokenisation of card details.

This article aims to scrutinize these regulations to observe the consistency of standards mandated across these regulations and identifying any ambiguities that might exist.

Analysis of the RBI's guidelines on payments systems

The first important regulation which was the inception point of data localisation was the directive on 'Storage of Payment System Data' issued in 2018. It was followed by issuance of FAQs in 2019 for better clarity.[2] This directive stated that the entirety of transaction payment data should be stored in a system 'only in India'. This move was aimed to prevent storing of payments transaction data overseas and also give RBI access to the said data, when required. Further, the directive also allowed processing of the data overseas in limited situations but mandated that the data should be deleted abroad and brought back to India within one business day or 24 hours from payment processing (whichever is earlier) and stored in India. Moreover, for cross border transaction data generated in a transaction with a foreign and domestic component, a copy of the domestic component was allowed to be stored abroad.

1 See: https://www.business-standard.com/finance/news/average-cost-of-data-breaches-in-india-hits-2-18-million-rbi-report-124072900610_1.html, (last accessed November 7, 2024).

2 See: https://www.rbi.org.in/commonperson/English/Scripts/FAQs.aspx?Id=2995, (last accessed November 7, 2024).

The second set of regulations was the guidelines on Payment Aggregators (PAs) and Payment Gateways of 2020. These guidelines stated that PAs and merchants were not permitted to store customer card data on their databases or servers accessed by merchants. The guidelines further specified that preventive measures should be adopted to ensure that the data was not stored in infrastructure belonging to external jurisdictions, and appropriate controls should be implemented to prevent unauthorised access to the data. These guidelines were followed by a clarification in 2021, which stated that merchant entities were not allowed to store payment data, irrespective of their PCI-DSS compliance, other than a limited amount of data for transaction tracking. However, an ambiguity emerged in the clarification: while the main guidelines restricted merchants from storing customer card data, the clarification was broader, extending the restriction to all forms of payment data (which goes beyond just customer card data).

The final piece of the regulatory framework was the introduction of tokenisation. Under this framework, tokenisation replaced actual card details with a unique token, reducing the risk of fraud by limiting the exposure of sensitive card information. The tokenisation guidelines mandated that only card issuers and card networks could store actual card data, with all previously stored card data required to be purged. However, entities were allowed to retain the last four digits of the card number and the card issuer's name for transaction tracking or reconciliation purposes.

Business Challenges

As transactions become increasingly global, complying with localisation requirements for end-to-end transaction data can be challenging. However, the mandated localisation could be minimised to focus only on necessary vigilance standards, such as localising card data. Notably, the upcoming Digital Personal Data Protection Act of 2023 also does not impose any data localisation requirements.

Furthermore, while these regulations focus on securing financial data through measures such as tokenisation and data localisation, they introduce several practical challenges for merchants and payment processors. Notably, there is ambiguity regarding the transfer of tokens to third parties and whether tokens are subject to data localisation requirements.

Additionally, the regulation limiting the storage of the last four digits of the card number and the card issuer's name for transaction tracking may not align with the needs of merchants, who often require additional information, such as customer names, BIN (Bank Identification Number) details, and card network names, to enhance customer service and implement fraud detection measures. Restricting access to these additional details could hinder efforts to combat fraud and identify potential risks in the payment ecosystem. Therefore, expanding the permissible data storage to include BIN and card network information would be beneficial.

Lastly, the rationale behind restricting regulated entities like Payment Aggregators from storing customer card data, especially when they are directly overseen by the RBI, is unclear. A more detailed explanation of this policy would help clarify its impact on the payment ecosystem and the role of PAs in protecting consumer card data.

— Huzefa Tavawalla and Palak Kapoor

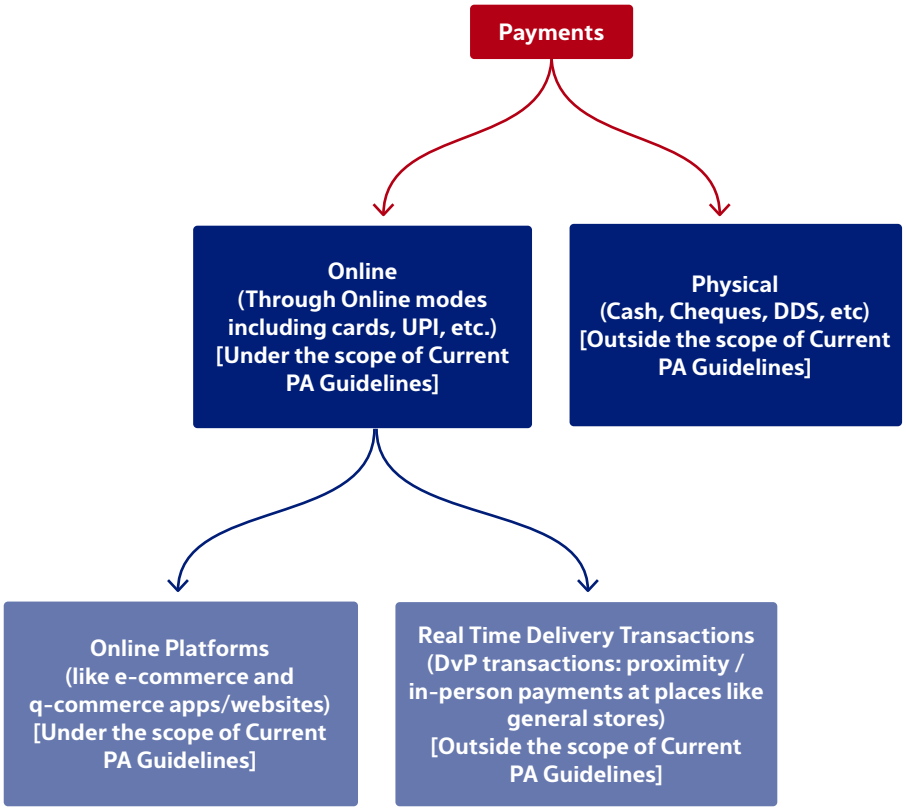
July 29, 2024

B. From Click to Brick: Proposal to Expand Payment Aggregator Guidelines for Online and Offline Transactions

Click the above logo to visit the published article

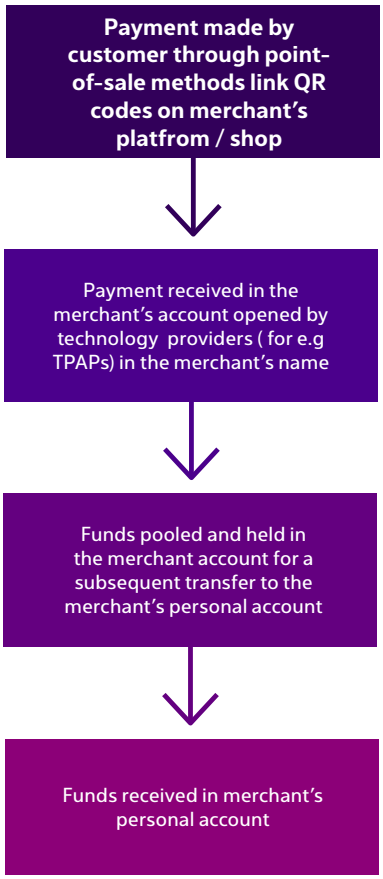
Earlier this year, the Reserve Bank of India (RBI) released draft directions proposing to amend the currently applicable Payment Aggregators guidelines issued on March 17, 2020 followed by clarifications on March 31, 2021 (PA Guidelines). The proposed draft directions largely intend to cover in-person payment options which will bring forth a significant change in the applicability of the PA Guidelines, especially in relation to various offline fintech business models (PA-P Circular).

As a background, the PA Guidelines define payment aggregators (PAs) in a manner that limits the scope of such entities to transactions in the online and e-commerce space. However, the PA Guidelines did not apply to Delivery vs Payment (DvP) transactions (DvP Exemption). While the scope of DvP transactions was not defined, on a holistic reading of the guidelines, DvP transactions were understood to be transactions involving payment for real-time delivery of a good and/or service. Below is an illustration of the scope of PA Guidelines, as applicable to various kinds of payments:



The intention behind the PA Guidelines was to provide for an actively regulated ecosystem for PAs involved in online payments but a lot of fintech models associated with offline / in-person payments were not always regulated. On September 30, 2022, the RBI released a Statement on Developmental and Regulatory Policies (Statement) wherein it was proposed to apply the PA Guidelines to entities involved in payments made during "*proximity/face-to-face transactions.*"

It has been reported that the lack of regulation of fintech models associated with offline / in-person payments led to issues including an increase in high-value one-time transactions at point-of-sale (POS) terminals, which may be due to merchants allowing individuals to undertake these transactions in exchange for cash. Entities aggregating payments made through POS terminals were largely unregulated by the RBI, since they did not fall under the scope of the PA Guidelines due to the DvP Exemption along with the agency exemption under the Payments and Settlement Systems Act, 2007 (PSA). Additionally, creative models including UPI-based third-party application providers implemented QR code-based payments where a "merchant account" was created for respective merchants by the technology service provider, and UPI payments were collected and settled with merchants on a periodic basis. An illustrative payment model involving UPI QR code is as follows:



As an analysis of the model illustrated above, technology companies have been (i) facilitating payments, (ii) enabling merchants to receive payments from customers, (iii) receiving payments from customers, (iv) pooling the funds, and (v) transferring the funds to the merchants after a specified period. However, it could be argued that technology companies in spirit may have been playing the role of a PA but remained unregulated based on the DvP Exemption and the PSA agency exemption.

Going forward, as per the draft PA-P Circular, RBI has not only expanded the scope of the definition of PAs, but has also diluted the DvP Exemption. Based on the draft PA-P Circular, *PAs are entities that facilitate aggregation of payments in online or physical point of sale payment modes through a merchant's interface (physical or virtual), and subsequently settle the collected funds to such merchants.* Further the draft PA-P Circular defines PA-P as PAs which facilitate face-to-face / proximity payment for DvP transactions.

Based on the above, DvP transactions that were previously exempted could be regulated, hence bringing real-time physical payments made in an online form, especially including POS and QR code payments within the scope of the PA Guidelines. However, cash-on-delivery payments continue to be exempted and outside the scope of the PA Guidelines.

While the Statement clearly mentions that the RBI seeks to synergize the regulation of PAs, it appears that one of the intentions behind the introduction of the draft PA-P Circular was to regulate technology companies that have been acting akin to PAs (by facilitating payments) without any authorization from the RBI. Once the draft PA-P Circular is implemented, various fintech companies involved in the payment ecosystem will now be required to seek authorization from the RBI and comply with requirements as applicable to existing PAs.

— Huzefa Tavawalla and Rhythm Vijayvargiya

December 20, 2023

C. RBI warms up to fintechs for cross-border e-commerce

Click the above logo to visit the published article

The Reserve Bank of India (RBI) is transforming the landscape of online e-commerce payments. With the introduction of the Regulations for Payment Aggregator – Cross Border (PA-CB Guidelines) on 31 October 2023, fintechs are now empowered to aggregate cross-border payments for the import and export of goods and services. This new framework marks a significant shift, offering fintechs a well-defined structure for cross-border transactions, which were previously limited.

Shift from bank-centric to inclusive e-commerce payments

Historically, authorized dealer (AD) banks dominated cross-border e-commerce payments. Fintechs were confined to serving as online payment gateway service providers (OPGSPs), limited to facilitating specific transactions under stringent arrangements with banks. This role did not encompass the actual handling or settlement of funds.

In April 2022, the RBI proposed a draft to overhaul the OPGSP model with online export-import facilitators (OEIFs), aiming for more inclusive processing and settlement of small value export and import payments. Although this draft is not yet law, it has set the stage for broader changes.

New horizons for non-bank entities in e-commerce

The PA-CB guidelines dramatically expand the role of non-bank entities in e-commerce transactions. These entities can now move beyond the traditional bank-dependent payment gateway model. They are enabled to manage escrow accounts and facilitate payments for a broader range of services, including imports, with more autonomy over settlement timelines.

Implications for existing payment aggregators

Existing Payment Aggregators (PAs) eyeing expansion into PA-CB services must first inform the RBI of their current and intended operations. This notification, required within 60 days of the PA-CB Guidelines' issuance, is a precursor to seeking RBI's approval for continuing or expanding their services.

Transition for existing cross-border payment facilitators

Entities like OPGSPs, previously playing a prominent customer-facing role, now face a new mandate. To continue in their capacity as cross-border e-commerce payment facilitators, they must acquire licences as PA-CBs, aligning with the new regulatory framework.

Adherence to anti-money laundering norms

In light of a July 2023 Delhi high court ruling, entities operating under the OPGSP model are now subject to the Prevention of Money Laundering Act (PMLA), 2002, reporting requirements. The PA-CB guidelines reinforce this mandate, requiring non-bank entities involved in cross-border payments to register with the Financial Intelligence Unit — India (FIU–IND) under the PMLA. Entities currently in this space have until 30 April 2024, to secure RBI authorization, necessitating early registration with FIU–IND.

New PA–CBs will be categorized as "reporting entities", hence requiring registration with the FIU–IND under the PMLA.

Challenges and opportunities in implementation

While adopting the PA guidelines' conditions, the PA-CB guidelines may encounter operational complexities. Practical aspects, such as settlement timelines and transaction mechanisms, need reconsideration for smoother integration into the intricate cross-border banking infrastructure.

— Purushottham Kittane and Huzefa Tavawalla

November 7, 2023

D. Indian Fintechs to go Global: New Payment Opportunities for Cross Border E-Commerce

Background

1. The RBI has introduced a new authorization framework for Indian entities seeking to aggregate cross-border payments by issuing Regulations for Payment Aggregator — Cross Border on October 31, 2023[3] (**"PA–CB Guidelines"**). These PA–CB Guidelines are applicable to entities involved in processing / settlement of crossborder payment transactions for import and export of goods and services.

2. Previously, the RBI had developed a framework through circulars in 2010[4], 2011[5], 2013[6] and 2015[7] allowing Online Payment Gateway Service Providers (**"OPGSPs"**) to enter into standing arrangements with Authorised Dealer (**"AD"**) Banks. Through such arrangements, OPGSPs were allowed to facilitate cross-border transactions for import of goods and software and export of goods and services, subject to monetary and other restrictions. Importantly, the role of OPGSPs did not extend to actual processing or settlement of funds which was handled by AD Banks.

3. In April 2022, the RBI had issued a draft circular on processing and settlement of small value Export and Import related payments facilitated by Online Export-Import Facilitators (OEIFs) which are intended to replace the OPGSP regulations.[8] Although, this circular has not been implemented as law.

4. Cross-border payments have also been subject to increased regulatory scrutiny in recent times:

   - In July 2023, the Delhi High Court had ruled that an entity operating as an OPGSP would also be subject to reporting requirements under India's anti-money laundering law i.e., the Prevention of Money Laundering Act, 2002 (**"PMLA"**).[9]

   - The recent amendments to the RBI Master Direction -Know Your Customer (KYC), 2016 (**"KYC Master Direction"**) in October 2023 requires regulated entities to undertake diligence measures and meticulous monitoring to identify accounts facilitating illegal cross-border transactions and report suspicious transactions to the Financial Intelligence Unit – India (**"FIU–IND"**).[10]

   - The RBI also issues an alert list of entities which are neither authorized to deal in forex under the *Foreign Exchange Management Act, 1999*[11]. The Directorate of Enforcement also has conducted investigations on networks facilitating illegal cross-border exchange.[12]

3 Available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12561&Mode=0, (last accessed November 4,2023).

4 Please see: https://rbi.org.in/Scripts/NotificationUser.aspx?Id=6107&Mode=0, (last accessed November 4, 2023).

5 Please see: https://rbi.org.in/scripts/NotificationUser.aspx?Id=6762&Mode=0, (last accessed November 4, 2023).

6 Please see: https://rbi.org.in/Scripts/NotificationUser.aspx?Id=8030&Mode=0, (last accessed November 4, 2023).

7 Please see: https://rbi.org.in/Scripts/NotificationUser.aspx?Id=10037&Mode=0, (last accessed November 4, 2023).

8 Available at: https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4118 (last accessed November 4, 2023).

9 W.P. (C) 138 of 2021. Please see our analysis of the judgment available at: https://nishithdesai.com/SectionCategory/33/Research-and-Articles/12/57/Hotline/10740/2.html, (last accessedNovember 4, 2023).

10 Please see: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12549&Mode=0, (last accessed November 4,2023).

11 Available at: https://rbi.org.in/scripts/bs_viewcontent.aspx?Id=4235, (last accessed November 4, 2023).

12 Please see: https://enforcementdirectorate.gov.in/sites/default/files/latestnews/Press%20Releasesearches% 20on%2019.06.2023_0.pdf, (last accessed November 4, 2023).

The Framework

The PA-CB Guidelines provide for eligibility criteria, authorization process, permitted accounts and other conditions for banks and non-banking entities facilitating cross-border payments for import and export of permissible goods and services. Some important conditions for non-bank entities are detailed below.

Authorization:

- Current PA–CBs: Any entity currently operating as a PA–CB must apply for authorization by April 30, 2024. These PA–CBs must register with the FIU-IND to apply for such authorization. Further, such PA-CBs must ensure adherence to the RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways dated March 17, 2020[13] **("PA Guidelines")** on governance, merchant on-boarding, customer grievance redressal and dispute management framework, baseline technology recommendations, security, fraud prevention and risk management framework within 3 months from the date of issuance of the PA–CB Guidelines (i.e., January 31, 2024).
- Current Payment Aggregators **("PAs")**: PAs which are currently authorized or have their authorization applications pending should first inform the RBI within 60 days of the issuance of the PA–CB Guidelines whether they have existing PA–CB operations and whether they would continue with it. If yes, PAs would need to seek approval of the RBI.
- Going forward: Any PA that intends to operate as a PA–CB or vice versa must obtain RBI approval before undertaking such activity.

Imports:

- Payments towards imports are to be made to the PA-CB's domestic escrow account, transferred to an Import Collection Account held with an AD category-I scheduled commercial bank and ultimately sent to the foreign merchant.
- PA-CBs are responsible for undertaking customer due diligence as per the KYC Master Direction of any offshore e-commerce marketplace, offshore PAs or offshore merchants directly onboarded.

Exports:

- Payments towards exports must be made to an Export Collection Account created separately for each currency with an AD category-I scheduled commercial bank, and then settled to the account of the merchant in India.
- PA-CBs are responsible for undertaking customer due diligence as per the KYC Master Direction of its Indian merchants who are directly onboarded, domestic e-commerce marketplaces or entities providing domestic PA services.

Other Conditions:

- PA-CBs facilitating either import and export transactions or both should ensure to not to facilitate payments for restricted / prohibited goods and services i.e., those not permissible under the prevailing Foreign Trade Policy.[14]

13 Available at: https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0, (last accessed November 4, 2023).

14 The Foreign Trade (Development & Regulation) Act, 1992 empowers the central government to notify a Foreign Trade Policy that applies to imports and exports of goods and services. The Foreign Trade Policy is updated from time to time and the current one i.e. the Foreign Trade Policy 2023 is effective from April 1, 2023. Please see: https://www.dgft.gov.in/CP/, (last accessed November 4, 2023).

- PA–CBs facilitating both import and export transactions should maintain separate collection accounts for such imports and exports, and also maintain a separate escrow account for domestic PA activity (if applicable).
- Net worth requirements for eligibility of applicants are similar to those prescribed under the PA Guidelines.
- Since PA–CBs maintain import and export collection accounts with AD banks, they are deemed as "designated payment systems"[15] which allows the RBI to prescribe maintenance of liquid assets as against the amounts collected from PA–CBs in future.
- PA–CBs facilitating import transactions should also undertake due diligence of the buyer if the value per unit of goods/services imported is more than INR 2,50,000.
- Other conditions from the PA Guidelines apply mutatis mutandis to PA-CBs.

Key Takeaways

1. **Non-bank entities permitted:** Cross-border commerce payments for e-commerce transactions were largely within the domain of AD banks. Fintechs were permitted to the limited extent of providing payment gateway services in the form of OPGSPs. However, these PA-CB Guidelines now open up opportunities for non-bank entities to provide such cross-border payment services for e-commerce transactions. Existing PAs too may find it a lesser leap to expand by providing PA-CB services and offer more expansive service bundles to their clients/merchants.
2. **Status of current cross-border payment facilitators:** Before the issuance of the PA-CB Guidelines, non-bank entities such as OPGSPs and collection agents performed a front-facing role with the customers/merchants and relied on the infrastructure of AD Banks in the background. However, such entities may now have to get licensed as PA–CBs to continue being the front-facing service providers for facilitating cross-border e-commerce payments.
3. **Liberalization of payments for import of services:** The existing OPGSP regulations did not allow OPGSPs to facilitate import of services except software. However, the PA–CB Guidelines allow transactions for import / export of all goods and services, subject to compliance of law. This is a welcome move for foreign merchants as they may be able to offer digital services to Indian consumers without actually setting up a physical presence in India.
4. **Registration with the FIU-IND:** Entities which are currently undertaking cross-border e-commerce payments such as OPGSPs and collection agents may need to register with the FIU-IND before seeking RBI approval for continuation of services. Other entities, once approved by the RBI to undertake PA–CB activity, may also be required to register with the FIU–IND.
5. **Operational complexities**: The PA-CB Guidelines adopt conditions of the PA Guidelines mutatis mutandis. However, implementation of certain conditions under the PA Guidelines such as settlement timelines and other mechanisms such as chargebacks, reversals, etc. should be evaluated for practical feasibility considering complexities of the underlying banking infrastructure for cross-border payments.

— Huzefa Tavawalla and Purushottham Kittane

15 As per section 23A of the Payments and Settlement Systems Act, 2007.

August 25, 2023

E. Fintechs to be Covered Under Anti-Money Laundering Laws: Indian Court Directs a Cross Border Online Indian Gateway to Register as a Reporting Entity!

The Delhi High Court **("DHC")** has ruled recently in a judgment pronounced on July 24, 2023[16] **("Judgment")** that a certain Cross Border Online Payment Gateways Service Provider **("Petitioner")** is a "Payment System Operator" [17] **("PSO")** under the Prevention of Money Laundering Act, 2002 **("PMLA")** despite not falling within the ambit of the definition of PSO (system provider) under the Payments and Settlements System Act, 2007 **("PSS Act")**.[18]Further, as a consequence of qualifying as PSO under the PMLA, the Petitioner will also be required to meet the obligations of a "Reporting Entity" **("RE")** including under Prevention of Money Laundering (Maintenance of Records) Rules, 2005 **("PMLA Maintenance Rules")**.[19] Pertinently, while reaching this conclusion, the DHC examined the specific function and role of an Online Payment Gateway Service Provider **("OPGSP")** and specifically of the Petitioner and how it "enabled" payments to qualify as a PSO. This Judgment of the DHC has been appealed by the Petitioner before a division bench of the same court.

In this piece, we examine the Judgment in light of the business model of the Petitioner. We will also look at the implications of the Judgment on other OPGSPs and intermediaries in the payment eco-system being regarded as reporting entities under the PMLA.

Petitioner's Case in Point:

Petitioner operates as a cross border OPGSP, and is regulated by the notification of the Reserve Bank of India **("RBI")** dated September 24, 2015 on Processing and settlement of import and export related payments facilitated by Online Payment Gateway Service Providers **("OPGSP guidelines")**[20]by entering into standing arrangements with Authorized Dealer Category-I Schedule Commercial Banks **("AD Banks")** such as Citibank and State Bank of India.

16 W.P. (C) 138 of 2021.

17 Section 2(1)(rc) of the PMLA defines a "payment system operator" as "a person who operates a paymentsystem and such person includes his overseas principal.Explanation.-For the purposes of this clause, "overseas principal" means,– (A) in the case of a person, being an individual, such individual residing outside India, who owns or controls or manages, directly or indirectly, the activities or functions of payment system in India; (B) in the case of a Hindu undivided family, Karta of such Hindu undivided family residing outside India who owns or controls or manages, directly or indirectly, the activities or functions of payment system in India; (C) in the case of a company, a firm, an association of persons, a body of individuals, an artificial juridical person, whether incorporated or not, such company, firm, association of persons, body of individuals, artificial juridical person incorporated or registered outside India or existing as such and which owns or controls or manages, directly or indirectly, the activities or functions of payment system in India."Section 2(1)(rob) of the PMLA defines a "payment system" as "a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them.Explanation – For the purposes of this clause, "payment system" includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations."

18 Section 2(1)(q) of the PSS Act defines a "system provider" as "a person who operates an authorized payment system." Section 2(1)(i) of the PSS Act defines a "payment system" as "a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange;Explanation.— For the purposes of this clause, "payment system" includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations."

19 Section 2(1)(wa) of the PMLA defines a reporting entity as "a banking company, financial institution, intermediary or person carrying on a designated business or profession."Section 2(1)(l) of the PMLA includes a "payment system operator" in its definition of a "financial institution."

20 Available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10037&Mode=0, (last accessed August 8, 2023).

Relevant to the current case, the Petitioner facilitated Indian exporters / sellers to receive cross-border payments from foreign remitters / buyers.

These remittances from foreign remitters are pooled into an offshore account and then remitted to an AD bank e.g., Citibank's NOSTRO collection account where the funds are held in USD. Thereafter, the funds are converted into INR into Citibank's export collection account in India and further disbursed to accounts of Indian exporters.

While the Petitioner had represented that the offshore account where foreign remitters' payments were pooled and transferred to the NOSTRO collection account was that of a "Global acquirer / aggregator", the Respondent, Financial Intelligence Unit India **("FIU–Ind")**, disputed such representation and contended as per information received from Citibank, the Global acquirer / aggregator is an "offshore account" of the Petitioner. The DHC did not reach a conclusive finding on this fact.

The Petitioner had filed the present petition before DHC challenging the order of the FIU-Ind dated 17 December 2020 holding it to be a RE under the PMLA and imposing monetary penalty of about INR 96,00,000 (USD 115,419 approximately) under section 13(2)(d) of the PMLA for the following alleged violations:

1. Section 12 of the PMLA for avoiding obligations of maintaining and reporting transaction records by not registering as RE under the PMLA;
2. Rule 7 of the PMLA Maintenance Rules for failure to register and communicate the name address of its principal officer;
3. Rule 7 of the PMLA Maintenance Rules for failure to register and communicate the name address of its Designated Director to FIU-Ind.

Before the DHC, the Petitioner argued that it was not a PSO under the PMLA and hence it will not qualify as RE as it provides a mere technological interface for export transactions and does not 'enable' transfer of funds between an Indian payee/exporter and an overseas payer/buyer. It stated that it is not involved in onboarding/enrolling of the overseas remitter/payer in this export transaction and only on boards the Indian payee/exporter which provides the payment link to this foreign entity. The onboarding of foreign remitter and transfer of funds is essentially done/handled and routed by the AD Banks at the end of each transaction.

Therefore, it argued that, it is the AD Banks and not the Petitioner which is involved in handling of funds, clearing, receiving payments and performing settlement activities. The Petitioner relied upon the (i) identical definition of 'payment system' under the PSS (save for the exclusion of a stock exchange) wherein payment gateways such as OPGSPs are not treated as PSOs; and (ii) an affidavit by the RBI in another case stating that OPGSPs such as the Petitioner are not a PSO under the PSS Act.[21]

Arguments Advanced by the FIU–Ind and RBI:

The Respondent, FIU–Ind, disputed the stance of the Petitioner and argued that the interpretation of the definition of 'payment system operator' under PMLA ought not to be equated to that under the PSS and has to be interpreted more expansively in light of the objectives of the PMLA legislation.

21 Abhijit Mishra v. Reserve Bank of India (W.P. (C) No. 7007 of 2019).

On facts, the Respondent argued that the Petitioner has certain information about the foreign remitter which the AD Banks are not privy to.

They argued that, this leads to FIU-Ind having 'impaired visibility' on such information thereby limiting/ hindering its function to effectively carry on anti-money laundering activities as against any suspicious transactions.

Opinion of The Committee Formed by Ministry of Finance:

As per directions passed by DHC on January 12, 2021, the Secretary, Ministry of Finance **("MOF")** constituted a committee, with a nominee of the RBI and the MOF, to clarify their position on whether entities involved in facilitating monetary transactions ought to be categorized as PSOs and thus, REs under the PMLA. The Committee reached the conclusion in the affirmative categorizing Cross-Border OPGSPs as PSOs and thus, REs under the PMLA.

Analysis of The DHC:

- **Pari Materia definition of payment system under the PSS Act and PMLA:**

  The DHC concluded that payment aggregators and OPGSPs are treated differently under the PSS Act. OPGSPs being technology providers does not appear to be regulated by (i.e., licensed under) the PSS Act even if they are involved in some capacity in the payment chain.The similarity of definitions between the PSS Act and the PMLA should not have a bearing since the objectives and the underlying legislative policy of how a payment system should be treated under the PMLA is different from that of the PSS Act. Under the PMLA, "payment system operator" should be interpreted to ensure effective implementation of its provisions and to avoid the spectre of the offender sneaking out of the "meshes of the law".

- **Petitioner as a "payment system operator" under the PMLA:**

  The DHC observed that the use of the word "enabling" in the definition of a "payment system operator" would capture any system which assists, makes possible or advances the objective of a payment between a payer and a beneficiary. Further, the word "involving" in the definition of a "payment system" would also mean any facet or feature comprised or comprehended in the course of a payment transaction. Hence, these interpretations would also apply to any participant in the payment chain who is not handling actual funds but nonetheless performs an important function.The DHC also notes that the objective of the PMLA is to prevent money laundering activities which would involve analysis of all the data points generated in a transaction. Since it was found that the actual remitter details were not initially made available to the AD Bank by the Petitioner (payments to the AD Bank were made from an "offshore" account purportedly of the Petitioner), the Petitioner was understood to be acting as a gatekeeper for such details which only the Petitioner had because of its onboarding relationship at the remitters' end. Hence, due to the above dual factors, the Petitioner was held to be a "payment system operator" under the PMLA. Interestingly, this finding was based on the PMLA alone and the court did not consider Petitioner's conduct/operations in other jurisdictions (where the Petitioner was offering more than a technology interface for payments).

- **Petitioner's business model distinguished from UPI Third-Party Application Providers:**

  The DHC laid down a fundamental distinction between the role of the Petitioner and a Unified Payment Interface **("UPI")** Third-Party Application Providers **("TPAPs")** such as Google Pay or Amazon Pay. It observed that unlike the UPI TPAPs, the Petitioner plays an active role in onboarding of foreign parties under the OPGSP framework. In the process of onboarding, the Petitioner maintains a nodal/ collection account with a Bank through which OPGSP funds are routed. The credits/debits in this nodal/collection account are made by the AD Banks on the instructions of the Petitioner. In the case of TPAPs however, the end-to-end transactions are undertaken from bank accounts of the transacting parties themselves and their details are already captured with AD Banks.

- **Discharge of the Penalty against the Petitioner:**

  In the order dated 17 December 2020, the FIU–Ind had imposed significant penalty on the Petitioner for a period of 32 months commencing from 16 March 2018 i.e., from the time when it had received notice for alleged violation of RE obligations under the PMLA. The DHC discharged the penalty obligations imposed by FIU–Ind on the basis that (i) the Petitioner had bonafide belief that it was not a PSO and as such did not deliberately act in violation of a statutory obligation. The stand taken by Petitioner would not amount to willful disobedience as the position of law on the aspect was unsettled. This was buttressed by the different stance taken by RBI and FIU–Ind; and (ii) the Petitioner had cooperated with the FIU–Ind at all stages even while disputing its status as an RE including suggesting different mechanisms to share information vide a letter to the FIU–Ind.

Takeaways:

- **Implication on payment "technology" intermediaries under the PMLA:**

  The Judgment is a defining interpretation and will likely result in additional obligations and compliance requirement for other entities performing similar functions as that of the Petitioners. Considering the decision, the following key points arise in the assessment of any technology service providers as PSOs under the PMLA:

  1. The technology provider does not necessarily have to be involved in handling of funds; and
  2. The role of the technology provider in onboarding the parties to the transactions as well as having access to details of the parties and transactions.

  Considering the varied functions that are performed by intermediaries such as the payment gateways, the role, function and actual involvement will have to be examined on a case-to-case basis. However, cross- border payment intermediaries may be more likely to be caught under this definition of PSOs under the PMLA, especially in cases where certain transaction details are only available with the payment intermediary and not available with AD Bank.

- **Applicability to Domestic Payment Gateways:**

  Domestic payment gateways, which are not licensed PSOs under the PSS Act, are less likely to be deemed as PSOs under the PMLA. This is because the transaction details in all likelihood will already be with the AD Bank or payment aggregators (who are licensed under the PSS Act to consummate online transactions).
  Thus, from the perspective of object and purposive interpretation, the intent of the PMLA stands fulfilled.

- **Qualifiers to be a PSO under the PMLA:**

  Who then can be interpreted as a PSO following the interpretation of the PMLA laid down in this Judgment? As observed by the DHC, should the determination of a PSO be:

  1. definition based – i.e., applies to any participant in the payment chain who is not handling actual funds but nonetheless performs an important function by enabling payments between a payer and a beneficiary? or
  2. function based – i.e., applies to participants in the payment chain because they have access to details of the parties and transactions to the exclusion of AD Banks?

  If the definition-based approach is taken, it may lead to all payment intermediaries (including domestic payment gateways) involved in any capacity to be determined as a PSO under the PMLA so as to not frustrate the objects of the PMLA. This may be viewed by many as an extreme interpretation, and may also hamper technological innovation by many tech service providers in this space. On the other hand, the function-based approach prods one to go beyond the applicability of the definition to assess nature of access to details that a payment intermediary has. These considerations should be done on a case-by-case basis.

- **Role of OPGSPs under the PSS Act:**

  The role of OPGSPs under the PSS Act is more straightforward and the Judgment has reiterated the position that an entity which does not handle actual funds is unlikely to be controlled under the PSS Act by the RBI. Hence, OPGSPs are not subject to licensing requirements under the PSS Act.

- **Understanding the FIU–Ind's role of enforcement under the PMLA:**

  It is clear from the FIU–Ind's arguments as well as the DHC's observations that the FIU–Ind's intention is for an RE to undertake monitoring and reporting obligations regarding all available and relevant data points in a payment transaction. In situations where the AD Banks have limited data points, non-licensed entities (such as the Petitioner in the current case) could be equally held responsible for data sharing/reporting. Information is supreme under the PMLA. Similarly, a question also arises at the end of AD Banks as to what extent they can/should require non-licensed entities to share transaction data points and avoid penalties for non-compliance as REs themselves.

- **Levy of penalties by the FIU–Ind:**

  Interestingly, even though the DHC ruled that the Petitioner was in fact a PSO under PMLA, it did not uphold the penalty imposed by FIU-Ind on the Petitioner. This is attributable to the strategy adopted by the Petitioner on its position under the PMLA, bona fide efforts to cooperate and no willful intention to disobey the law.

- **Other future implications:**

  The implications of the Judgment would also have to be looked through the lens of payment policy developments in this space in India. In 2022, the RBI published draft guidelines for Processing and settlement of small value Export and Import related payments facilitated by Online Export-Import Facilitators (OEIF)[22] **("OIEF Guidelines")** which is intended to replace the OPGSP guidelines. The OIEF Guidelines propose revisions to the parameters of payment transactions allowed, modes of collection, and what can be debited and credited in the collection accounts. Based on the interpretation of a PSO as per the Judgment, Online Export-Import Facilitators may also be subject to the PMLA.
  However, this would need to be evaluated on a case-by-case basis.

— Aishwarya Jain, Purushotham Kittane, Arjun Gupta, Alipak Banerjee and Huzefa Tavawalla

22 Available at: https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4118, (last accessed August 8, 2023).

June 23, 2023

F. Cross-Border Unified Payments Interface (UPI) Transactions: Connecting India with the World

THE NATIONAL LAW REVIEW

Click the above logo to visit the published article

Introduction

India has risen as the topmost country for digital payment transactions in recent years. Last year, India recorded more digital payment transactions than those in the US, China and Europe combined.[23] This is thanks to the Unified Payments Interface **('UPI')** introduced by National Payments Corporation of India **('NPCI')** about seven years ago on April 11, 2016. Every month, the number of UPI transactions continue to surpass those of the previous month.

According to the NPCI, for the month of May 2023, the total number of monthly UPI transactions reached a record 9.4 billion with the transaction value of record INR 14.89 trillion (about USD 181 billion).[24]

India's rise as the global leader in digital payments is attributable to its robust technological infrastructure and timely regulatory interventions. As UPI enables instant mobile-to-mobile payments at practically no cost, millions of people have adopted it as the primary mode of payments. Every UPI transaction is required to use two-factor authentication, a passcode or PIN for accessing any UPI app as well to confirm the transaction. Thus, UPI has become a highly secure payment mechanism earning trust among its users.

Recently, India has undertaken various initiatives to extend the reach of UPI beyond its borders and make it a truly global payment system. We have described below the Indian and country-wise initiatives on cross-border and international UPI payment facilities.

23 Available at: https://www.ndtvprofit.com/business/indias-digital-transactions-more-than-that-of-us-china-europe-combined-trade-official-3860293, (last accessed June 16, 2023).

24 Available at: https://www.npci.org.in/what-we-do/upi/product-statistics, (last accessed June 6, 2023).

India Initiatives

NPCI is a non-profit umbrella organisation set up by the Reserve Bank of India **('RBI')** that operates retail payments and settlement systems in India. Since 2020,[25] NPCI has taken several steps to enable the use of UPI globally for international peer-to-peer and merchant payments.

UPI Global

The NPCI mandated that all stakeholders – i.e. member banks, third party application providers and other payment providers – provide UPI Global by December 31, 2021.[26] While this timeline was extended to September 30, 2022 to accommodate additional members that had not implemented the feature at the issuer and UPI app level[27], no further extension has been granted by NPCI. PhonePe was the first Indian fintech to support cross-border UPI payments. Users of PhonePe can pay through their Indian bank accounts to merchants at merchant outlets or points-of-sale in the UAE, Singapore, Mauritius, Nepal, and Bhutan.[28] Paytm has also announced that it will launch support for UPI Global payments. [29]

UPI for Non-Resident Indians

As per NPCI's circular dated January 10, 2023[30], non-resident accounts like Non-Resident External **('NRE')** and Non- Resident Ordinary **('NRO')** Accounts with international mobile numbers are allowed to be on-boarded and transact using UPI. To begin with, mobile numbers from the following ten countries would be permitted - United States, United Kingdom, Singapore, Canada, Australia, Oman, Qatar, UAE, Saudi Arabia and Hong Kong. The responsibility of adherence to foreign exchange laws and RBI guidelines is on member banks, and anti-money laundering compliance is the responsibility of the remitter and beneficiary banks.

UPI for Foreign Travellers in India

The RBI Master Directions **('PPI MD')** on Prepaid Payment Instruments **('PPIs')** were amended in February 2023.[31] laying down provisions for issuance of PPIs to foreign nationals and NRIs visiting India (together, 'Travellers'). The PPI MD states that INR denominated21 full-KYC PPIs can be granted to Travellers, beginning with those travelling to India from G20 countries. Inbound travellers to India can avail UPI facilities through PPIs issued to them. To begin with, this facility has been offered to inbound travellers from G20 countries for merchant payments at select international airports -- New Delhi, Mumbai and Bengaluru airports.[32]

25 NPCI international merchant acceptance circular dated September 4, 2020, not available in public domain; referenced in the NPCI September 2021 circular.

26 NPCI September 2021 circular, available at: https://www.npci.org.in/PDF/npci/upi/circular/2021/UPI-OC-117-International-merchant-payments-acceptance-through-UPI-UP.pdf, (last accessed June 6, 2023).

27 NPCI April 2022 circular, available at: https://www.npci.org.in/PDF/npci/upi/circular/2022/UPI-OC-146-Compliance-timeline-for-International-Acceptance-using-UPI-(UPI-Global).pdf, (last accessed June 6, 2023).

28 Available at: https://economictimes.indiatimes.com/nri/invest/phonepe-launches-support-for-cross-border-upi-payments/articleshow/97821018.cms, (last accessed March 9, 2023)

29 Available at: https://bwdisrupt.businessworld.in/article/Paytm-To-Roll-Out-UPI-International-Aims-Catering-Indian-Diaspora/10-05-2023-476002/, (last accessed June 6, 2023).

30 NPCI January 2023 circular, available at: https://www.npci.org.in/PDF/npci/upi/circular/2023/UPI-OC-161-Extension-to-UPI-Circular-No-60-Crediting-Debiting-Non-Resident-accounts-in-UPI.pdf, (last accessed March 9, 2023).

31 Available at: https://m.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156, (last accessed March 9, 2023).

32 Available at: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR1765UPIEA2CDA20100B4AD2B666805A5BCDAD1E.PDF, (last accessed March 9, 2023).

Currently, ICICI Bank, IDFC First Bank and two non-bank issuers, Pine Labs Private Limited and Transcorp International Limited, issue UPI-linked wallets. In February 2023, EbixCash was the first entity to provide UPI services to the travellers as part of a pilot testing phase.[33]

Traveller PPIs are issued in the form of e-wallets linked to UPI, after physical verification of the Travellers' passports and visas. Traveller PPIs can only be loaded/reloaded against the receipt of foreign currency in cash or through any other payment instrument, and the Traveller PPIs can only be used for merchant payments. The amount outstanding on the Traveller PPI cannot be more than INR 200,000 at any given time.

Bilateral Initiatives

Several digital economies such as the UK, Singapore and UAE have partnered with India's NPCI, through the latter's wholly owned subsidiary, NPCI International Payments Limited **('NIPL')**. The partnerships propose to offer seamless cross-border payments, allowing Indians to use UPI in Singapore for real-time peer-to-peer and merchant transactions, and in the UK and UAE for real-time peer-to-merchant transactions.

Singapore

Singapore has been actively promoting its Payments Roadmap that covers initiatives such as common QR codes for accepting payments, unified points of sale, and PayNow.[34]

The RBI and the Monetary Authority of Singapore announced in September 2021 that they would link their fast payment systems i.e., UPI and PayNow respectively.[35]Chia Ling Koh, Managing Director at Osborne Clarke Singapore, remarks: "UPI – PayNow is currently offered by DBS and non-bank payment institution Liquid Group. The Monetary Authority of Singapore has been issuing non-bank payment institution licences under the relatively new Payments Services Act. Without a doubt, the payments services market is getting competitive in Singapore."

The UPI - PayNow linkage should enable fund transfers between users in India and users in Singapore. The transfers from users in India to those in Singapore can be done using mobile phone numbers, and from Singapore to India using UPI virtual payment addresses. Further, Indian users visiting or living in Singapore can make payments to merchants in Singapore using their bank UPI apps.[36]

Peer-to-peer transactions

The UPI - PayNow linkage was operationalised in February 2023.[37] The account holders of participating banks and financial institutions in Singapore and India can undertake cross-border remittance transactions via UPI and PayNow.

33 Available at: https://www.outlookmoney.com/news/ebixcash-launches-upi-pilot-for-foreign-nationals-visiting-india-during-g20-news-262211, (last accessed March 9, 2023).

34 Available at: https://www.mas.gov.sg/development/e-payments, (last accessed June 6, 2023).

35 Available at: https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52223 and https://www.mas.gov.sg/news/media-releases/2021/ singapores-paynow-and-indias-upi-to-link-in-2022, (last accessed June 6, 2023).

36 Available at: https://www.nets.com.sg/nets/for-business/accept-overseas-wallets-foreign-cards#faq, (last accessed January 4, 2023).

37 Available at: https://www.rbi.org.in/commonperson/English/Scripts/FAQs.aspx?Id=3415, (last accessed March 9, 2023).

As per the RBI FAQs on the UPI-PayNow linkage,[38] six Indian banks[39] are currently enabled for receiving remittances through the linkage, and four Indian banks[40] are currently enabled to send the remittances. The FAQs list the apps and platforms offered[41] by the above-mentioned banks that can be used as long as a user's UPI ID is registered with the bank. There are two participating entities from Singapore[42] for receiving and sending remittances.

A daily transaction limit of INR 60,000 (about SGD 1,000) is applicable, and presently, only peer-to-peer remittances for the purposes of maintenance of relatives abroad & gifts are allowed. The RBI's Liberalised Remittance Scheme **('LRS')** limit of USD 250,000 per financial year per individual will be applicable. P2M transactions have not been enabled via on the linkage. The linkage allows real time transactions, similar to domestic UPI transactions.

Users should be able to commence using this feature when the participating banks roll-out an update in their respective UPI apps. As of June 2023, we were unable to locate the payment and receiving feature on certain listed apps.

Peer-to-merchant transactions

For peer-to-merchant transactions, UPI is accepted in Singapore by select merchants via BHIM, the mobile payment app developed by NPCI based on the underlying UPI infrastructure. BHIM is linked to PayNow, and Indian users in Singapore can pay using BHIM UPI by scanning QR codes at select merchants in Singapore. The UPI feature on apps from the following banks can be used by Indians for cross-border merchant payments using PayNow: City Union Bank, UCO Bank, Bank of Baroda and Punjab & Sindh Bank. At the time of payment, the BHIM app will automatically convert and display the amount from Singapore Dollars to Indian Rupees, for ease of reference for the Indian payer. The transaction rate applicable for using UPI at a merchant (through the NETS QR code) is 1.8% of the transaction value.[43]

UAE

NIPL has collaborated with various institutions in the UAE such as Mashreq Bank's subsidiary NeoPay[44], the Arab Monetary Fund through Buna[45] (a cross-border payment system), and Network International, an organization enabling digital commerce in the MENA region.[46] These partnerships aim to help implement payment solutions that will lead to interoperability with UPI, and help Indians make seamless payments to merchants in the UAE. NeoPay has begun accepting payments through BHIM UPI across NeoPay enabled shops and merchant stores. Additionally, PhonePe has enabled UPI transactions at merchant stores and points of sale in the UAE. This will help with peer-to- merchant payments for Indians in the UAE.

38 Ibid.

39 The six Indian banks are Axis Bank, DBS Bank India, ICICI Bank, Indian Bank, Indian Overseas Bank and the State Bank of India.

40 The four Indian banks are ICICI Bank, Indian Bank, Indian Overseas Bank and the State Bank of India.

41 The apps that can be used for receiving remittances are Axis Pay by Axis Bank, DBS Digibank by DBS Bank India, ICICI iMobile by ICICI Bank, IndOASIS by Indian Bank, BHIM IOB Pay by Indian Overseas Bank, BHIM SBI Pay by State Bank of India. Similarly, the apps that can be used for sending remittance include IndOASIS by Indian Bank and BHIM SBI Pay by State Bank of India, while the Indian Overseas Bank and the ICICI Bank offer internet banking services for the same.

42 The two participating entities are DBS Bank and Liquid Group.

43 Available at: https://www.nets.com.sg/wp-content/uploads/2022/06/document-application-optin-rupay-b*him.pdf, (last June 6, 2023).

44 Available at: https://www.npci.org.in/PDF/npci/press-releases/2022/NIPL-Press-Release-BHIM-UPI-goes-live-at-NEOPAY-terminals-in-UAE.pdf, (last accessed August 12, 2022).

45 Available at: https://www.amf.org.ae/en/news/10-03-2022/arab-monetary-fund-amf-signs-mou-npci-international-payments-limited-nipl, (last accessed August 12, 2022).

46 Available at: https://economictimes.indiatimes.com/news/international/uae/npci-arm-network-int-join-hands-for-upi-payment-system-in-uae/articleshow/87784172.cms, (last accessed June 6, 2023).

UK

The UK has set up Faster Payment System **('FPS')** with private participation of payment start-ups that enable real time payments online or via telephone banking, of up to GBP 1 million.[47] The NIPL signed a memorandum of understanding with PayXpert to enable acceptance of UPI in the UK.[48] This collaboration is to enable Indian bank account holders to use UPI through PayXpert's point of sale devices in the UK for in-store payments, including through UPI-based QR code payments. This partnership is expected to provide Indian travellers with a familiar and convenient way to make payments in the UK.

Bhutan, Nepal... and the World

In similar efforts, the NPCI collaborated with Bhutan early on, with Bhutan being the first country to adopt UPI standards for its QR code deployment, and the first country to accept mobile based payments through BHIM.[49]

Further, in furtherance of India's Neighbourhood First Policy, Nepal adopted UPI for their digital transactions in February 2022. NIPL joined hands with Gateway Payments Service and Manam Infotech to provide the services in Nepal, for both peer-to-peer and merchant payments.[50] PhonePe currently has enabled peer to merchant payments through UPI in Nepal and Bhutan.

NIPL has also set its eyes on partnerships with global private fintech players. It joined hands with TerraPay, a global payments infrastructure company, by signing an MOU that will allow Indian residents with a UPI ID to receive real- time international payments through TerraPay[51]. NIPL signed a similar MOU with PPRO, to enable offering of RuPay card and UPI acceptance across PPRO's global clients such as payment service providers (PSPs) and global merchant acquirers.[52]

NPCI is presently working towards enabling cross-border transactions with several other countries. It aims to collaborate with at least 30 more countries including Australia and France.[53] Significantly low costs and the secure mechanism for conducting UPI-based digital transactions is likely to benefit many developing countries too, as they aspire to establish digital financial infrastructure to build a globally integrated digital economy.

47 Available at: https://www.wearepay.uk/what-we-do/payment-systems/faster-payment-system/, (Last accessed June 18, 2023).

48 Available at: https://www.npci.org.in/PDF/npci/press-releases/2022/NPCI-Press-Release-India%E2%80%99s-NPCI-International-signs-PayXpert-as -UK%E2%80%99s-first-acquirer-for-UPI-and-RuPay.pdf, (last accessed January 4, 2023).

49 Available at: https://pib.gov.in/PressReleasePage.aspx?PRID=1735075#:~:text=Bhutan%20is%20the%20first%20country,payments%20through%20t he%20BHIM%20App, (last accessed June 6, 2023). .

50 Available at: https://www.hindustantimes.com/world-news/nepal-to-become-first-country-to-deploy-india-s-upi-platform-101645148414811.html, (last accessed June 6, 2023).

51 Available at: https://www.livemint.com/companies/news/terrapay-npci-international-partner-to-enable-real-time-international-payments-11643278725965 .html, (last accessed June 6, 2023).

52 Available at: https://timesofindia.indiatimes.com/business/international-business/npci-arm-uk-fintech-to-take-upi-global/articleshow/99829891.cm s?from=mdr, (last accessed June 6, 2023).

53 Available at: https://inc42.com/buzz/india-to-provide-upi-to-the-world-in-talks-with-30-countries-it-minister/, (last accessed August 12, 2022).

Legal Considerations

Data Storage

The RBI's circular on 'Storage of Payment System Data' dated April 6, 2018[54] **("DL Circular")** acknowledged safety and security measures required in digital payments. It mandated that all payment system providers and banks must store data relating to payment systems operated by them only in India. Complete end-to-end transaction details should be part of the data stored.[55] For the foreign leg of the transaction, the data may be stored in the foreign country.

Further, processing of payment transactions outside India may be carried out.

1. In such case, the data may be stored outside India during such time but should be stored only in India after the processing,
2. Wherein processing is done outside India, the data should be deleted from the systems abroad and brought back to India no later than 1 business day or 24 hours from the payment processing, whichever is earlier,
3. Subsequent activities such as settlement processing after the payment processing, if done outside India should be done on a real-time basis and the data should be stored only in India during such process, and
4. In case of any other related processing activity, such as chargeback, etc., the data can be accessed, at any time, from India where it is stored.

Though the DL Circular does not specifically mention UPI within its scope, the DL Circular should apply to cross- border UPI transactions. This is because the NPCI is authorised by the RBI as a retail payments organisation, and the DL Circular should apply to the NPCI and the bank members that are a part of the NPCI and that process UPI transactions. The DL Circular has been previously enforced by the NPCI against all digital payment platform members in May 2020, requiring the members to submit system audit reports to demonstrate compliance with the DL Circular.[56]

Foreign Exchange Control

In India, all transactions involving foreign currency are controlled by the Foreign Exchange Management Act, 1999 **('FEMA')**. FEMA treats "capital account transactions" separately from "current account transactions." Current account transactions, under the Section 2(i) of FEMA, are transactions that include "payments due in connection with foreign trade, other current business, services, and short-term banking and credit facilities in the ordinary course of business" and "remittances for living expenses of parents, spouse and children residing abroad"[57] UPI transactions are typically undertaken for purchase of goods, services, or peer-to-peer payments, and not for purchase of assets such as immovable property. Therefore, peer-to-peer and merchant UPI Global transactions are likely to fall under current account transactions.

54 RBI circular on 'Storage of Payment System Data', 2018, available at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244, (last accessed June 6, 2023).

55 See Response to question 5: https://m.rbi. org.in/scripts/FAQView.aspx?Id=130, (last accessed June 6, 2023). End-to-end transaction details and information pertaining to payment or settlement transaction that is gathered / transmitted / processed as part of a payment message / instruction includes: Customer data (Name, Mobile Number, email, Aadhaar Number, PAN number, etc. as applicable), payment sensitive data (customer and beneficiary account details); Payment Credentials (OTP, PIN, Passwords, etc.), and Transaction data (originating & destination system information, transaction reference, timestamp, amount, etc.).

56 Available at: https://www.livemint.com/news/india/npci-starts-auditing-data-localisation-norms-for-digital-payment-firms-11589260599583.html, (last accessed June 6, 2023).

57 Section 2(j), Foreign Exchange Management Act, 1999.

UPI Global transactions would fall under the LRS limit for resident individuals of USD 250,000 per financial year,[58] and should not be exempt from the limit unless specifically exempted by amendment of the Foreign Exchange Management (Current Account Transactions) Rules, 2000 **('Current Account Rules')**. For example, the erstwhile Rule 7 of the Current Account Rules had exempted international credit card transactions made when the card holder is outside India from requiring prior RBI approval and had kept such transactions outside the LRS limit. This rule was omitted by way of amendment in May 2023[59].

While there are no restrictions imposed by the NPCI circulars on what UPI Global may be used for, as on date, the cross-border UPI transactions can be used for peer-to-peer remittances for gifts and maintenance of relatives abroad.[60] If UPI cross-border transactions are classified as current account transactions, future UPI Global transactions should be permitted under the Current Account Rules, unless:

1. The transactions are prohibited, such as remittances from lottery winnings, racing / riding income or any other hobby, remittances towards lottery tickets, sweepstakes, banned/proscribed magazines, foot-ball pools etc., remittance for payment of commission on exports made towards equity investment in joint ventures/ wholly owned subsidiaries abroad of Indian companies, remittance of dividend by any company to which the requirement of dividend balancing is applicable, etc.[61]
2. The transactions require prior approval of the Government of India such as remittances towards cultural tours,[62] or
3. The total remittances of the individual in a financial year exceed the limits under LRS.[63]

Conclusion

The promotion and acceptance of UPI by a variety of countries demonstrates that cross-border transactions using UPI are only set to grow. This is in furtherance of the acceptance of RuPay cards in Singapore and the UAE[64], and the Bharat Bill Payment System (BBPS) that will soon be able to accept cross-border inward payments.[65] The RBI Annual Report 2022 also provides recommendations in relation to cross-border UPI such as geotagging of existing payment touchpoints and expanding literacy initiatives.[66]

The benefits of enabling cross-border UPI payments include:

1. ease of remittances from and to India, for countries where peer-to-peer payments are enabled, as in the case of Singapore,
2. ease of payments for Indian residents visiting other countries, such as tourists and short-term visitors,
3. ease of transactions for Indian students studying abroad, and

58 See response to Question 11, Linkage FAQs, available at: https://www.rbi.org.in/commonperson/English/Scripts/FAQs.aspx?Id=3415, (last accessed June 6, 2023).

59 Foreign Exchange Management (Current Account Transactions) (Amendment) Rules, 2023, available at: https://egazette.nic.in/WriteReadData/2023/245899.pdf, (last accessed June 6, 2023).

60 Please see response to Question 8, available at: https://www .rbi.org.in /commonperson/English/Scripts/FAQs.aspx?Id=3415, (last accessed June 6, 2023).

61 Rule 3 read with Schedule I of the Foreign Exchange Management (Current Account Transactions) Rules, 2000.

62 Rule 4 read with Schedule II of the Foreign Exchange Management (Current Account Transactions) Rules, 2000.

63 Rule 5 read with Schedule III of the Foreign Exchange Management (Current Account Transactions) Rules, 2000.

64 Available at: https://www.neopay.ae/en/home/; https://www.nets.com.sg/faqs/business/accept-foreign-cards-and-payments/, (last accessed August 12, 2022).

65 Available at: https://www.business-standard.com/article/economy-policy/bbps-inward-payments-to-deepen-cross-border-payment-ecosystem-in-india-12 2080501149_1.html, (last accessed August 12, 2022).

66 Available at: https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?year=2022, (last accessed August 12, 2022).

4. ease of shopping from merchants outside of India, without requiring international payments through debit/credit cards, in countries where the collaboration extends beyond point-of-sale machines.

While agreements have been entered into with various countries and entities in foreign countries, effective implementation on-ground and proliferation of UPI usage may take some time and may need to overcome some teething issues. UPI has changed the way payment transactions are happening in India. Within a short-span of few years, India's cash-based economy is rapidly transitioning to a digital transaction economy. Such society- transforming innovations have global benefits. The partnerships with established international payment service providers indicate a positive push to enable access to UPI for potential users across the world. In addition, the reach of UPI is aiding India's push to internationalize the rupee. This is a great step towards India's globalisation efforts and could establish India as a truly global digital economy.

— Aaron Kamath & Mihir Parikh

The authors thank Akhileshwari Anand for her efforts and contribution to this publication.

April 26, 2023

G. New Legal Framework for Outsourcing of IT Services in India's BFSI Sector

Background

The Reserve Bank of India **("RBI")** issued the Master Direction on Outsourcing of Information Technology Services **("Outsourcing Directions")**[67] on April 10, 2023. This was following RBI's Statement on Developmental and Regulatory Policies released with its bi-monthly Monetary Policy Statement dated February 10, 2022,[68] wherein it expressed concerns regarding the outsourcing of Information Technology **("IT")** services by regulated entities such as banks and non-bank financial companies, and the associated financial, operational and reputational risks. The Draft Master Direction on Outsourcing of IT Services was issued in June 2022 **("Draft Directions")**[69] pursuant to which these Outsourcing Directions were introduced as law.

Timeline for compliance with the Outsourcing Directions:

Type of Outsourcing Arrangement	Compliance with the Outsourcing Directions
Existing Agreement	
Agreements up for renewal prior to October 1, 2023	By April 10, 2024
Agreements up for renewal on or after October 1, 2023	By April 10, 2026
New Agreements	
Agreements in effect prior to October 1, 2023	By April 10, 2024
Agreements in effect on or after October 1, 2023	From the date of the agreement

As on date, there are existing directions or guidelines regulating outsourcing by different regulated entities of the RBI such as banks,[70] co-operative banks,[71] and non-banking financial companies **("NBFCs")**[72](together "**Existing Outsourcing Frameworks**"). While these directions or guidelines regulate outsourcing by the above-mentioned entities, the Outsourcing Directions specifically address outsourcing of IT services of banks, NBFCs, credit information companies and certain financial institutions **("REs")**[73].

67 Accessible at: https://m.rbi.org.in/Scripts/NotificationUser.aspx?Id=12486&Mode=0, (last visited April 12, 2023).

68 Accessible at: https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53248, (last visited April 12, 2023).

69 Accessible at: https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4156, (last visited April 12, 2023).

70 RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, 2006, accessible at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=3148&Mode=0, (last visited April 12, 2023).

71 RBI Guidelines for Managing Risk in Outsourcing of Financial Services by Co-operative Banks, 2021, accessible at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12123&Mode=0, (last visited April 12, 2023).

72 RBI Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs, 2017, accessible at: https://rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=11160, (last visited April 12, 2023).

73 The Outsourcing Directions are addressed to banking companies (including corresponding new banks and SBI),primary co-operative banks, non-banking financial companies (NBFCs), credit information companies and All India Financial Institutions such as NHB, NABARD, SIDBI, EXIM Bank and NaBFID.

The purpose of these Outsourcing Directions is to ensure that outsourcing arrangements neither diminish an RE's ability to fulfil its obligations to customers nor impede effective supervision by the RBI.

Applicability

The Outsourcing Directions are only applicable to arrangements entered into for Material Outsourcing of IT Services by REs.[74] 'Outsourcing of IT Services' includes outsourcing of IT infrastructure management, maintenance and support, network and security solutions and maintenance (hardware, software or firmware), services and operations related to data centres, and management of IT infrastructure and technology services associated with the payment system ecosystem.

Material Outsourcing of IT services are those services that, if disrupted or compromised, would have the potential to:

- make a significant impact on the RE's business operations, or;
- have a material impact on the RE's customers in the event of any unauthorized access, loss, or theft of customer information.[75]

The Outsourcing Directions are not applicable to certain services and vendors, which illustratively include: (1) services that are not considered 'Outsourcing of IT Services',[76] such as corporate internet banking services, external audit such as vulnerability assessment/penetration testing, SMS gateways, off-the-shelf software products under license, payroll processing, and procurement of IT hardware; and (2) vendors who are not considered as 'Third-Party Service Providers', such as business correspondents, payment system operators[77], co-branding fintech partners, telecom service providers, and IT security and audit consultants.[78]Where REs avail cloud computing services and outsource security operations center services, there are additional requirements prescribed under the Outsourcing Directions such as cloud adoption policy and security measures, disaster recovery and incident response, audits, adequate oversight, physical access in certain areas, etc.[79]

74 Clause 2(c), Outsourcing Directions: '"Material Outsourcing of IT Services" are those which: a) if disrupted or compromised shall have the potential to significantly impact the RE's business operations; or b) may have material impact on the RE's customers in the event of any unauthorised access, loss or theft of customer information.'

75 Clause 3(a)(ii), Outsourcing Directions.

76 Clause 3(a)(iv), Outsourcing Directions: '"Outsourcing of IT Services" shall include outsourcing of the following activities: a) IT infrastructure management, maintenance and support (hardware, software or firmware); b) Network and security solutions, maintenance (hardware, software or firmware); c) Application Development, Maintenance and Testing; Application Service Providers (ASPs) including ATM Switch ASPs; d) Services and operations related to Data Centres; e) Cloud Computing Services; f) Managed Security Services; and g) Management of IT infrastructure and technology services associated with payment system ecosystem.'

77 Authorised under the Payment and Settlement Systems Act, 2007.

78 Appendix III.B, Outsourcing Directions. This includes: "i. Vendors providing business services using IT. Example – BCs, ii. Payment System Operators authorised by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for setting up and operating Payment Systems in India iii. Partnership based Fintech firms such as those providing co-branded applications, service, products (would be considered under outsourcing of financial services), iv. Services of Fintech firms for data retrieval, data validation and verification services such as (list is not exhaustive): a. Bank statement analysis b. GST returns analysis, c. Fetching of vehicle information, d. Digital document execution, e. Data entry and Call centre services, v. Telecom Service Providers from whom leased lines or other similar kind of infrastructure are availed and used for transmission of the data, vi. Security/ Audit Consultants appointed for certification/ audit/ VA-PT related to IT infra/ IT services/ Information Security services in their role as independent third-party auditor/ consultant/ lead implementer".

79 Appendix I and II, Outsourcing Directions.

Key Obligations Under the Outsourcing Directions

Due Diligence: The Outsourcing Directions require that REs must evaluate the need for outsourcing based on the criticality of the activity, the expectations/outcome from outsourcing, the success factors and cost-benefit analysis, and the model for outsourcing. Adequate due diligence must be performed including any past experience of the service provider to whom services are to be outsourced by the RE (**"Service Provider"**), financial soundness and ability to undertake commitments under adverse conditions, business reputation and culture, and external factors such as political, economic, social and legal environment of the jurisdiction of the Service Provider.

Governance: Outsourcing of any activity would not diminish the responsibilities of the RE, its board or senior members in any way, who will be ultimately responsible for the outsourced activity. Therefore, the RE should make sure that the Service Provider employs the same standard of care (that should be high) in performance of the activities as the RE would have undertaken if the activity had not been outsourced.

Additionally, the RE should also make sure that in case the Service Provider is not a group company, it should not be owned or controlled by any directors, key managerial personnel, or approver of the outsourcing arrangement of the RE, or their relatives. However, this requirement can be done away with board approval and proper disclosures, oversight and monitoring of such an arrangement. The REs should have a board-approved outsourcing policy in place covering all necessary roles and responsibilities and criteria for outsourcing activities. The policy should also include disaster recovery, termination processes and exit strategies, including business continuity, of the outsourcing framework. The Outsourcing Directions also provide for specific responsibilities for the board, the senior management and the IT function of the RE.

Grievance Redressal: The RE should maintain a grievance redressal mechanism which should not be compromised in any manner owing to the outsourcing.

Outsourcing Agreement: REs are required to have a legally binding written agreement with each Service Provider. The outsourcing agreement should be sufficiently flexible to allow the RE to retain adequate control over the outsourced activity or the right to intervene with appropriate measures. The agreement should also clearly bring out the nature of the relationship between the RE and the Service Provider.

Further, the Outsourcing Directions provide for certain set of key provisions that should be in the outsourcing agreements which include, amongst others, proper definitions of the services, monitoring and assessment, sub- contracting upon prior consent, and contingency plans.
The REs must ensure that the regulator must have the authority to perform inspections of the Service Provider as well as the sub-contractors, and the authority to access the RE's infrastructure and data that is stored or processed by the Service Provider and its sub-contractors.

The Service Provider should also be obliged to comply with any directions issued by the RBI in relation to the outsourced activities and other applicable laws including the Information Technology Act, 2000. The outsourcing agreement must also cover data-related aspects such as applicable data localization requirements as per applicable law, provision of details of data processed and shared with customers of the RE and other parties, the Service Provider's liability to the RE in the event of a confidentiality/security breach, etc.

Risk Assessment and Exit: The Outsourcing Directions also provide that REs must carry out risk assessments and maintain a risk management framework as they are responsible for the activities of the Service Provider to their customers including incidents in relation to cybersecurity incidents, confidentiality and integrity of information, etc. REs must ensure that incidents, including cyber incidents and those resulting in disruption of service and data loss/leakage, are reported to them by the Service Provider without undue delay, in order to enable the RE to report the incident to the RBI within 6 hours of detection by the Service Provider. This has been changed from the Draft Directions, that required immediate reporting and no later than one hour of detection.

A management framework for monitoring and control of outsourced activities including service uptime, service levels, and certifications are prescribed. REs are also required to audit Service Providers regularly in relation to the outsourced activity, by external or internal auditors. The Outsourcing Directions also permit pooled audit of a Service Provider by REs that avail services from the same Service Provider, as long as the audit requirements are met effectively.

Outsourcing Within a Group

Agreements executed for IT services being outsourced to a group entity are required to be done based on a board- approved policy, with appropriate service level arrangements/agreements with the group entity. The choice of the group entity should be based on objective reasons as would be used for choosing a third party, and all dealings should be at an arm's length basis.[80]

Cross Border Outsourcing

In cases of cross-border outsourcing, the RE should also closely monitor the policies of the Service Provider's jurisdiction on a continuous basis and set up mitigation measures based on the country's risk. Further, the governing law of the arrangement can be agreed upon between the RE and Service Provider, and should be clearly specified. REs and the RBI should have the right to audit Service Providers based outside India, even in case of liquidation of the Service Providers.

Key Takeaways

Existing guidelines: While the Existing Outsourcing Framework regulates outsourcing of various non-core activities of REs, including of financial services, the Outsourcing Directions are specific to outsourcing of IT services. The Existing Outsourcing Framework may continue to apply alongside the Outsourcing Directions to REs, depending on the scope of the outsourcing activities. It is to be noted that the Outsourcing Directions do not apply to payment system operators, to which the RBI Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators, 2021 will apply.

80 Clause 20, Outsourcing Directions.

Applicability of the Outsourcing Directions: While the Outsourcing Directions are drafted as applicable only to arrangements entered into for Material Outsourcing of IT Services by REs[81], an issue that may arise is the determination of materiality. The definition of 'Material Outsourcing of IT Services' is very wide and leaves scope for interpretation by the REs, and it is unclear what parameters REs are expected to follow to determine materiality.

More importantly, there are no specific obligations in the Outsourcing Directions applicable to 'Material Outsourcing of IT Services'. The obligations mentioned across the Outsourcing Directions are drafted for Outsourcing of IT Services. 'Outsourcing of IT Services' is wider in definition than 'Material Outsourcing of IT Services'.

For example, Chapter III of the Outsourcing Guidelines that deals with the governance framework requires a board- approved IT outsourcing policy for all REs intending to outsource any of its activities. Similar provisions are also elsewhere in the Outsourcing Guidelines which broadly apply to Outsourcing of IT Services (and not Materially Outsourcing of IT Services).

Practically, it is likely that REs would take a stance that the obligations under the Outsourcing Guidelines would be applicable to all Outsourcing of IT Services. Given that certain obligations are significant in terms of the powers given to the REs and RBI, such as the right to audit and control measures, Service Providers may have to undertake significant changes to adhere to such requirements. Also, REs may see pushback from Service Providers on inclusion of such clauses on the ground that the same may not amount to material outsourcing.

Renewal and New Agreements: REs would also have to revisit their existing outsourcing agreements and re- examine outsourcing arrangements, especially for REs with a multi-jurisdictional presence due to the cross-border related provisions. REs would also have to ensure that such agreements are renewed in line with the Outsourcing Directions' obligations and within the timeline prescribed for adherence. REs looking to enter into new outsourcing arrangements will have to closely evaluate the outsourcing agreement requirements under these Outsourcing Directions, and ensure the requirements are adhered to within the time period provided for applicability of the Outsourcing Directions.

Impact on Service Providers: Given the heightened level of compliance required by REs under the Outsourcing Directions, several compliances may be passed on to Service Providers by REs, to meet REs' own compliance with the law. The approach, proposed contractual wordings and extent of compliance passed on may differ from RE to RE viz the Service Providers.

Certain compliances that may be contractually imposed on Services Providers include audit rights for the RE and RBI, data storage norms and confidentiality, immediate cyber incident reporting, and RE's flexibility to amend certain terms of the agreement as part of its risk management. IT service providers should be mindful when negotiating their arrangements with REs, and understand what the RE may be legally required to ask of them, and what may be excessive and above the scope of the Outsourcing Directions.

– Akhileshwari Anand, Aaron Kamath & Huzefa Tavawalla

81 Clause 2(c), Outsourcing Directions.

April 2, 2023

H. Digital Lending in India: Analysis and Implications

Click the above logo to visit the published article

Introduction

Digital lending, via websites and apps, has changed the way customers borrow money, by combining technological advancement with traditional banking services. This has led to seamless borrowing, faster loan disbursal with minimum paperwork, and expanded access to credit to a larger group of people, with digital lending growing multi-fold during the Covid-19 pandemic. For example, various non-bank websites and apps offer instant loans, with loans being disbursed in less than 10 minutes and without any collateral. 'Pay-later' platforms have also helped people shop online without having to make upfront payments.

The Reserve Bank of India **("RBI")** chose to examine the functioning of digital lending apps and websites due to concerns of mis-selling to unsuspecting customers, data privacy breaches, misuse of data collected, hidden costs, unethical business conduct (including recovery agents resorting to harassment) and illegitimate operations. The RBI Working Group[82] was set up in January 2021 **("Working Group")**. The Working Group identified three major issues: conduct, technology and charges, based on which the Working Group released its recommendations[83] in November 2021 **("Recommendations")**.

The RBI Implementation[84] of the Recommendations was released in August 2022, and on September 2, 2022, the RBI released the Digital Lending Guidelines[85] **("Guidelines")**. The Guidelines have been issued under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934, the National Housing Bank Act, 1987, the Factoring Regulation Act, 2011 and the Credit Information Companies (Regulation) Act, 2005. Subsequent to this, the RBI published Frequently Asked Questions[86] to the Guidelines on February 15, 2023 **("FAQs")**.

This article explores the provisions of the Guidelines and its industry impact on 'buy now pay later' and first-loss default guarantee models and payment aggregators.

82 See: https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=50961.
83 See: https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189.
84 See: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR689DL837E5F012B244F6DA1467A8DEB10F7AC.PDF.
85 See: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=12382&Mode=0.
86 See: https://www.rbi.org.in/Scripts/FAQView.aspx?Id=155.

Brief Overview of the Guidelines

Applicability

The Guidelines are applicable to digital lending services extended by banks and non-banking financial companies (including housing finance companies) **("Regulated Entities" or "REs")**. It is clarified that the scope of digital lending would extend to lending activities that involve some physical interface with the borrowers, such as in customer acquisition, credit assessment, loan approval, disbursement, recovery, and associated customer service.

The Guidelines also refer to Digital Lending Apps **("DLA")** and Lending Service Providers **("LSP")**. DLAs are mobile and web-based applications with a user interface that facilitates digital lending services, (for example, the mobile banking app of a bank that enables a user to avail of a loan through their phone). A DLA can either be operated by an LSP or by an RE directly. LSPs are intermediaries between the RE and the borrower. LSPs are entities that act as an agent of the RE and carry out one or more of the RE's functions, such as customer acquisition, underwriting support, pricing support, servicing, monitoring, recovery of specific loans or loan portfolios.

The Guidelines reiterate that any outsourcing by an RE to an LSP or a DLA does not diminish the RE's obligations to conform to the existing RBI guidelines on outsourcing. In addition, REs also need to ensure that LSPs and DLAs comply with the Guidelines.

The Guidelines are applicable to fresh loans to existing customers and new customers, who are onboarded from September 2, 2022. For existing digital loans, that is, the loans that have been sanctioned as on September 2, 2022, REs were given time until November 30, 2022, to put in place adequate systems and processes to ensure compliance with the Guidelines.

Customer Protection

The Guidelines state that the loan disbursal and repayment cannot occur through an account of any third party, such as a pass-through account or a pool account, including accounts of LSPs and DLAs. The disbursals and repayments shall be made directly between the RE and the borrower's bank account, except in the following cases:

- Disbursals covered exclusively under statutory or regulatory mandate,
- Money flow between REs for co-lending transactions, for both priority and non-priority sector lending,
- Disbursals for specific end use, provided the loan is disbursed directly into the bank account of the end-beneficiary,
- When physical interface may be used for recovery of delinquent loans (only where absolutely necessary), or
- Repayment of loans issued as advances against salary, wherein the corporate employer of the borrower deducts the EMI amount from the salary payable, and repays the instalment directly to the RE.

Additionally, every RE should have and should ensure that their LSPs have a nodal grievance officer for addressing any issues with respect to digital lending, fintech and DLAs.

If a complaint lodged by the borrower against an RE or LSP engaged by the RE is not resolved by the RE within 30 days, the borrower can lodge a complaint on the Complaint Management System portal under the RBI-Integrated Ombudsman Scheme **("RB–IOS")**, or for entities currently not covered under RB-IOS, as per the grievance redressal mechanism prescribed by the RBI.

Disclosures

The Guidelines mandate that the RE must provide a Key Fact Statement **("KFS")** in a standard format. The KFS is required for all digital lending products, and must include the all-inclusive cost of the digital loan shown as an annual percentage rate, recovery mechanism, and details of the grievance redressal officer designated to deal with digital lending and fintech-related matters. Any charge or fee not mentioned in the KFS cannot be charged to the borrower.

The KFS shall also include the right of a borrower to have a cool-off/lookup period, during which the borrower can exit the digital loan by paying back the principal and proportionate annual percentage rate (that may include a one-time processing fee) without any penalty. REs are required to ensure that digitally signed documents on the letterhead of the RE, such as the KFS, the sanction letter, etc., shall be sent automatically to borrowers on their registered and verified email or phone numbers as SMSs, upon execution of the loan contract or transaction.

REs are required to ensure that any charges payable to the LSPs are paid by the RE to the LSP, and not charged by the LSP to the borrower. Further, any penal interest or charges levied on borrowers by the RE should be based on the loan's outstanding amount, and the rate of such penal charges should be disclosed upfront in the Key Fact Statement.

REs must publish the list of LSPs and DLAs engaged by them, and the details of their activities, on the RE's website. DLAs of REs and LSPs shall prominently display product and loan-related information at the on-boarding stage, to ensure borrower awareness. REs shall provide the borrower with the details of the LSP acting as its recovery agent, at the time of loan sanction and while passing on the recovery responsibilities to an LSP or changing of an LSP. If the borrower fails to repay the loan and a recovery agent has been assigned to the borrower, the RE must communicate the recovery agent's contact information to the borrower before the recovery agent contacts the borrower. REs must ensure that DLAs of the REs and LSPs have links (in a prominent, single place on their websites) to the REs' website where detailed information about the loan products, the lender, the LSP, particulars of customer care, etc., can be accessed by the borrowers.

The reasoning behind introducing such disclosure-related compliances is: (1) to ensure customers are informed about all charges applicable to them, and (2) for customers to be able to identify recovery agents of the RE, and ensure recovery agents may be held accountable for unethical practices. The concern with digital lending platforms was primarily the hidden charges in loans offered, with news reports stating[87] that certain platforms charged 35-40% as platform fees, service charges and processing fees. The concern appears to continue to post the Guidelines as well, as the Ministry of Electronics and Information Technology has blocked over 94 loan apps.[88]

87 See: https://timesofindia.indiatimes.com/business/india-business/online-lending-platforms-offering-loans-at-exorbitant-rates-hc-asks-rbi-to-file-status-report/articleshow/90690138.cms.

88 See: https://economictimes.indiatimes.com/tech/technology/non-chinese-lending-apps-including-payus-lazypay-kissht-blocked-on-meitys-order/articleshow/97656552.cms.

Data Protection

Data collection by LSPs should be need-based, with the explicit consent of the borrower at every stage. Explicit consent is required from the user for sharing their information with third parties. Most personal information collected by LSPs and DLAs should not be stored, except some basic minimal data such as name, address, and contact details of the customer that may be required to carry out the LSP and DLA operations. Further, phone data of the borrower, such as files, media, contact list, call logs, etc. must not be accessed. However, one-time access for the camera, microphone, location or any other facility necessary for on-boarding and/or KYC requirements is permitted, only with the explicit consent of the borrower. Further, no biometric data can be stored or collected in the systems of the DLA and LSP of REs.

The RE also has the responsibility to ensure that all the DLAs and LSPs that they engage have a comprehensive privacy policy, including details of third parties that may be allowed to collect personal information through the DLAs, the type of data that can be stored, length of storage, limitation of use of data, etc., and that the privacy policy is prominently disclosed by the DLAs and LSPs of the RE on their website or apps. All the data collected must be localized, i.e., it should be stored in servers located within India. Lastly, REs have the responsibility to ensure the privacy and security of the customer's personal information.

The RBI historically has included data protection and localization related provisions in its regulations, and this trend continues in the Guidelines. The restriction on data collected and the localization requirement under the Guidelines are due to:

- Excessive data and permissions[89] collected from borrowers by DLAs/LSPs, including by legitimate Indian fintechs offering digital lending. For example, several apps require users to provide permissions to access location, camera and contacts to use the app, although such permissions are not relevant to the services offered by the apps.
- The misuse of borrower data by several DLAs/LSPs. News reports state that over 300 digital lending apps[90] were used by cybercriminals in India to access user data and to harass borrowers.

Reporting and Due Diligence

REs shall ensure that any lending through DLAs and/or LSPs of the REs is reported to Credit Information Companies **("CIC")**, irrespective of the nature of the loan or its tenor. Digital lending products offered by REs or their LSPs over merchant platforms, involving short-term, unsecured or secured credits, or deferred payments, need to be reported to CICs by the REs as well.

REs are required to conduct enhanced due diligence before partnering with a LSP for digital lending. This diligence should include the LSP's technical abilities, data privacy policies, storage systems, fairness in conduct with borrowers and ability to comply with regulations and statutes. REs are also required to undertake periodic reviews of the conduct of LSPs, and guide LSPs on how to act responsibly if they are acting as recovery agents.

These due diligence provisions come in the light of several lending apps[91] operating with harsh and predatory lending and recovery practices.

89 See: https://www.itsecurityguru.org/2022/12/02/predatory-loan-apps-on-apple-app-store-and-google-play-extorting-victims/.

90 See: https://timesofindia.indiatimes.com/gadgets-news/heres-how-cybercriminals-are-using-nearly-300-loan-apps-to-steal-your-data/articleshow/95936269.cms.

91 See: https://www.livemint.com/news/india/chinese-lending-apps-mha-asks-states-uts-to-take-urgent-action-predatory-apps-11667133970624.html.

By imposing the obligation on REs to vet the LSP before partnering with them, the instances of such lenders operating in the digital lending industry may become significantly lower.

Industry Concerns

The Guidelines and the FAQs appear to plug the gaps identified in relation to the regulation of digital lending. However, the Guidelines in terms of practical implementation, require further details or clarifications. The industry-related concerns can be categorized as follows:

First Loss Default Guarantee

First Loss Default Guarantee **("FLDG")** is an arrangement between a fintech and an RE, wherein the RE issues the loan to the borrower, and the fintech promises to compensate the RE to a certain extent if the borrower defaults in repayment. FLDG is provided at a certain pre-decided rate. Until the Guidelines, REs such as banks and NBFCs would lend through fintechs and rely on the fintech's underwriting for the FLDG.

The FLDG cover motivated REs to offer more loans, which has previously put banks in a tight spot[92] at the time of recovery, with over 10% loans not being repaid on time in 2020. It appears that the Guidelines would require REs accepting such FLDGs to adhere to the provisions of the RBI Master Direction on Securitisation Of Standard Assets, specifically on synthetic securitization. The provision appears to prohibit any transfer of risk by an RE to a third party in relation to lending.

This issue has not been clarified in the FAQs. The industry, including LSPs, continues[93] to await RBI clarifications on whether FLDGs can be offered to REs or not. The industry is exploring alternative models such as revenue sharing based on repayment proficiency of loan portfolios, and revenue sharing of interest income between the fintech and the RE.

Payment Aggregators

PAs, as per the RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways[94], are "entities that facilitate e-commerce sites and merchants to accept various payment instruments from the customers for completion of their payment obligations without the need for merchants to create a separate payment integration system of their own." PAs facilitate merchants to connect with acquirers. In the process, they receive payments from customers, pool and transfer the payments to the merchants after a particular time period.

The issue faced by PAs in relation to the Guidelines is that some PAs have also been performing the functions of LSPs. For instance, the PAs were facilitating loans and pooling funds for disbursal and acceptance, including facilitating equated monthly installments **("EMI")** on e-commerce and digital platforms. The Guidelines have now restricted PAs (as PAs are not REs) from pooling money from borrowers and lenders. Thus, funds cannot pass through the accounts of PAs.

92 See: https://www.moneycontrol.com/news/business/fldg-once-popular-among-fintech-lenders-could-haunt-them-as-defaults-loom-5960901.html.

93 See: https://www.financialexpress.com/economy/rbi-ban-on-fldg-arrangement-fintechs-explore-alternative-models-to-meet-rbi-norms/2987194/.

94 See: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0.

This has been confirmed by the FAQs, which state that PAs performing the role of an LSP must comply with the Guidelines, and no express exception has been provided for PAs to handle funds in the digital lending process.

For example, in a "pay-later" option offered while making a payment on an e-commerce website, if the PA were handling funds directly, the transaction would have included a pass-through of funds through the PA account at the time of loan disbursal and repayment by the borrower-purchaser. The model so far was that some e-commerce platforms had an arrangement with REs for capital; when a customer opted for the pay later option, a digital loan could be availed immediately through banks or NBFCs, and loans would be disbursed through the PA's pooling account. Post the Guidelines and FAQs, money cannot pass through the PA's account.

Certain PAs may also offer both: (1) PA services to merchants, and (2) digital lending services to merchants (through partner banks or NBFCs). In this model, the partner bank or NBFC may directly disburse loans to the merchants. The PA collects money from the merchant's customers. The money collected is then apportioned by the PA between: (1) the merchant's account with the PA (for settlement of money collected from customers), and (2) the merchant's loan account with the bank or NBFC, as repayment of the merchant's loan. In this model, the issue that arises is that the PA may handle funds directly in loan repayment. Post the introduction of the Guidelines and the FAQs, the PA cannot handle the funds directly in the loan repayment.

Further, lending platforms have been struggling[95] to comply with the Guidelines to route loan repayments directly to the RE's account. As the model is dependent on customers, i.e. it requires linkage of the customer's bank accounts with the RE's account, this has been difficult for fintechs and REs to implement.

Against the backdrop of the Guidelines, the Payments Council of India **("PCI")** has made a representation[96] to the RBI to exempt PAs from the norm of the Guidelines that restricts fund flow of loan disbursals and repayments through pass-through accounts. PCI's reasoning was that PAs are regulated by the RBI, and the movement of funds is also through a regulated escrow account of PAs; hence, PAs should have the right to disburse loans and collect loan repayments through their regulated accounts. The PCI had also stated that the new Guidelines would hamper the operations of REs and increase their operational costs. However, the FAQs have clarified that while PAs offering only PA services would remain outside the ambit of the Guidelines, any PA performing the role of an LSP is required to comply with the Guidelines. No exemption, as sought by the PCI, is provided to PAs.

The significance of the restriction of pass-through of funds through the accounts of PAs is that several fintechs are now restricted from offering services that involve pass-through of funds through their pool accounts. Although the Guidelines are for lending activities, it appears to place a restriction on licensed PAs from participating in the process. Though PAs are RBI-authorised companies, this pass-through account restriction is not exempt for PAs under the RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2021.

'Buy Now Pay Later' Apps

Prior to the Guidelines, the RBI circular on Prepaid Payment Instruments **("PPIs")** and credit lines (June 2022) banned the loading of non-bank PPIs such as prepaid cards and wallets from credit lines.

95 See: https://www.livemint.com/companies/news/fintechs-get-on-the-job-to-comply-with-rbi-lending-norms-11670426761491.html.

96 See: https://www.moneycontrol.com/news/business/exempt-payment-aggregators-from-bank-account-norm-in-digital-lending-payments-council-to-rbi-9140501.html.

Credit lines are pre-approved borrowing amounts provided by banks or NBFCs (as lenders), that allow individuals and businesses to access credit anytime without further approval within the pre-approved borrowing limit. Basis the RBI's Master Direction on PPIs[97], PPIs such as e-wallets may only be loaded and reloaded using cash, debits to a bank account, and credit and debit cards, thus confirming that PPIs may not be loaded through credit lines.

This credit lines restriction affected several 'Buy Now Pay Later' **("BNPL")** platform providers, as the BNPL platforms offered credit to their users through non-bank issued PPIs, that used pre-approved credit-lines to load the PPIs. Prior to the restriction, loans were offered in real time or within minutes of the borrower's request, as the credit-lines were pre-approved and the borrower did not require further approval at the time of availing the BNPL service.

The RBI restriction on credit lines led BNPL companies to move to a model of fresh sanction of a loan for every lending transaction undertaken by the borrower on the platform. The new model requires the loan to be approved, disbursed and subsequently loaded into the PPI at each instance. This has led to a change in the operations of several such BNPL platforms.

The Guidelines further required changes by BNPL platforms to ensure there was no pass-through of loan disbursal or repayment through the BNPL platform account or any other intermediary account. The double whammy of the credit lines circular and the Guidelines has rendered the operations of BNPL companies in their erstwhile form virtually impossible. This has led to several such fintech companies having to undertake drastic pivots[98], and in certain cases, shutdown.

Conclusion

Despite the Guidelines being comprehensive in relation to customer and data protection, there remain industry-level concerns that require clarification for effective implementation. The clarification on the role of PAs has brought much-awaited clarity, and the RBI's stance is that pass-through of funds for digital lending through PAs and BNPL platforms is not permitted. Limited exemptions for corporate employers and physical recovery of loans have been provided, as explained above.

Industry players expect RBI to issue further clarifications[99] on the Guidelines, especially for the exemptions on offering FLDGs. Such a clarification would help the industry devise the right model to operate effectively and within the confines of the law. The pertinent factor for devising models relating to FLDGs is how REs may be motivated to lend digitally through LSPs/DLAs, if REs are not permitted to enter into FLDG arrangements with fintechs. Apart from industry bodies, the new Department of Fintech could liaise with fintechs and represent them before other relevant RBI departments to achieve a quick resolution on the FLDG issue.

— Akhileshwari Anand, Aaron Kamath, & Huzefa Tavawalla

97 See: https://m.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156.

98 See: https://www.business-standard.com/article/finance/ppi-norms-why-rbi-is-no-fan-of-fintechs-buy-now-pay-later-model-122062800115_1.html.

99 See: https://www.financialexpress.com/economy/rbi-ban-on-fldg-arrangement-fintechs-explore-alternative-models-to-meet-rbi-norms/2987194/.

January 18, 2022

I. No Internet? No Problem, as Indian regulator enables offline digital payment

Background

In a significant boost for offline digital transactions, the Reserve Bank of India (RBI) has released a framework[100] for facilitating small value digital payments in offline mode. An 'offline digital payment' is a transaction that does not require the internet or telecom connectivity. The framework, effective from January 3, 2022 is expected to boost digital transactions in areas with no or poor internet or telecom connectivity, particularly in semi-urban and rural areas in India.

As per the RBI's '*Statement on Developmental and Regulatory Policies*'[101], three pilots were successfully conducted in different parts of India to test small-value transactions. Based on the feedback, the RBI thought it fit to introduce such solutions and a framework suitable for conducting retail digital payments in offline mode throughout India. This is the first framework of its kind to enable digital payments sans the internet.

Framework

Authorized payment system operators, payment system participants and banks that are interested to provide or enable such payment solutions for their users may facilitate small value digital payments as per the following criteria:

1. The framework applies to payments made face-to-face (in proximity) using any mode or instrument like cards, ewallets, mobile devices etc.
2. Offline payments may be made subject to a limit of INR 200 (approx. USD 3) per transaction and an overall limit of INR 2,000 (approx. USD 30) for all offline transactions. The user limit may be replenished only through online mode.
3. Such transactions require user consent, though no additional factor of authentication is required such as a pin or one-time-password sent to the user's email address or phone number.
4. Users are entitled to similar protection against customer liability in case of fraudulent / unauthorized transactions and grievance redressal, as for regular electronic banking transactions.
5. Transaction alerts may be sent to the user after a time-lag, and though not necessary to be sent for each transaction, when sent they should provide details of each previous transaction.
6. The acquirer should absorb liabilities arising from any technical or transaction security issues at the merchant's end.

100 Available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12215&Mode=0., (Last accessed: January 15, 2022).

101 Available at: https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52368., (Last accessed: January 15, 2022).

Analysis

Boost for digital payments

In a sector which saw about 6 billion debit and credit card transactions at an amount of USD 174 billion and almost 5 billion prepaid instrument transactions (e-wallets, gift cards etc.) at an amount of USD 27 billion in FY 2020-21,[102] enabling digital payments in an offline mode is set to significantly boost digital payments in the country. Though the new framework may not have a significant impact on digital payments in metro or tier one cities in India, it should in the semi-urban and rural parts of India. Though telecom and internet connectivity in semi-urban and rural India is picking up, there is still some catching up to do. For instance, the Union Minister for Electronics, IT and Communication stated in Parliament in March 2021 that 25,067 villages in India lack mobile and internet connectivity.[103] In such places, the framework proposes to have a huge impact as it would enable people to transact in person through their cards, e-wallets and mobile without internet connections.

Pilot testing a welcome step

It is a welcome and encouraging takeaway that the RBI had tested the proposed solutions through three pilotprograms conducted over the course of about a year in different parts of India. Basis the feedback, the RBI thought it prudent to roll out the framework. This appears a well-planned and thought-out approach and sets a precedent for RBI and an example for other industry regulators to consider piloting proposed product and technology solutions before issuing enabling framework for its implementation in the sector.

Infrastructure considerations

The framework appears clear on the compliance requirements and criteria for implementation of the framework by banks and payment system operators. The RBI has not mandated specific technological solutions. Presumably, this may be left to the industry players to develop, test and deploy relevant product solutions to enable their users to transact in offline mode.

We would need to watch for instance, whether debit cards currently in use can be used for offline payments; or whether fresh debit cards would need to be issued that would be compliant for use in offline mode. For instance, cards with specific radio frequency identification (RFID) technology were issued to make them compliant for nearfield communication (NFC) contactless payments.

Reference to mobile device is interesting as one of the possible solutions. Banks and payment service providers may work out some solutions of embedded software with device companies. Banks, payment service providers and perhaps card networks may need to discuss and work with telecom and internet service providers on aspects such as processing payments through point-of-sale (PoS) terminals, mobile devices etc. either with or in the absence of network, and communicating transaction alerts to the user upon the user receiving connectivity.

102 Source: https://www.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=20737., (Last accessed: January 16, 2022).

103 See: https://www.thequint.com/news/hot-news/25067-villages-in-india-lack-internet-connectivity-prasad-in-ls., (Last accessed: January 15, 2022).

Implementation uncertainties

The framework is left to the banks and payment system operators to implement, at their 'desire' and is not a mandatory obligation placed on them. Given recent trends, for instance the new recurring payments e-mandate registration framework that took effect in October 1, 2021 (after multiple extensions), banks have been slow in developing and deploying technology solutions and infrastructure, and may also take a back-seat in implementing offline payments for their users, especially if not adequately incentivised. It would be interesting to observe if RBI continues the push for offline payments and ultimately mandates the banks and payment system operators to implement the framework.

Kirana shops the winner

In a world increasingly dominated by the internet and e-commerce, this step appears to benefit the *'kirana'* shops or local family-run shops, grocers and vendors the most. With an abundance of them in semi-urban and rural India where mobile data and internet connectivity may be infrequent, low or absent, footfall at such shops are bound to increase if consumers can transact through their card, mobile or e-wallet in offline mode for small value purchases like household items and groceries.

The framework may also benefit local merchants and vendors in such regions that facilitate low value mobilerecharges, lottery ticket sales, wallet reloading and sale of gaming or content related vouchers. Such transactions, that may typically be settled in cash by the consumer, could be done offline via the user's card, e-wallet or mobile device.

— Aaron Kamath & Gowree Gokhale

December 8, 2021

J. Regulations on E-Wallets, Gift Cards and Vouchers Given a Facelift

Click the above logo to visit the published article

Introduction

In a significant update, the Reserve Bank of India **("RBI")** released the Reserve Bank of India Master Directions on Prepaid Payment Instruments, 2021 **("PPI Regulations")**[104] in August, 2021. The PPI Regulations subsume the Reserve Bank of India (Issuance and Operation of Prepaid Payment Instruments) Directions, 2017 **("2017 Regulations")**[105] with immediate effect, and also consolidate various circulars on pre-paid instruments **("PPIs")** that had been issued between 2017 and 2021. These regulations are issued by the RBI under the Payment and Settlement Systems Act, 2007.[106]

More commonly referred to as 'e-wallets' or 'gift cards', PPIs are payment instruments that can be used for the purchase of goods or services against this stored value. The PPI Regulations impact products such as e-wallets, gift cards and vouchers, money transfer wallets, meal vouchers, metro/travel rail cards, etc. Where the 2017 Regulations allowed paper PPIs in the limited instance of prepaid paper meal vouchers (Sodexo being the best example), the PPI Regulations do not allow any form of paper PPIs.

Key Aspects of The PPI Regime

Important aspects of the now consolidated PPI regime are as follows:

I. Closed System PPIs Not Regulated by RBI

The 2017 Regulations classified PPIs into Closed System PPIs (used to facilitate the purchase of goods and services from that entity only), Semi Closed PPIs (used for purchase of goods and services, including financial services, remittance facilities, etc., at a group of clearly identified merchant locations),and Open PPIs (issued only by banks and are used at any merchant).

104 https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156, (last accessed November 30, 2021).

105 You may refer to our analysis on the 2017 Regulations here.

106 The PPI Regulations are issued under Section 18 read with Section 10(2) of the Payment and Settlement Systems Act, 2007.

The PPI Regulations retain the classification of Closed System PPIs and clarify that "the issuance or operation of such instruments is not classified as a payment system requiring approval / authorization by RBI and are, therefore, not regulated or supervised by RBI". This clarity will be welcomed by the industry as there existed divergent views on whether Closed System PPIs were required to comply with the terms of the 2017 Regulations even though they did not require authorization. Therefore, Closed System PPIs, i.e. any PPIs that are issued and redeemed by the same entity are not regulated by the RBI, and do not need to seek authorization to be offered.

II. Introduction of Small and Full PPIs

Where Closed System PPIs are issued and redeemed by the same entity, there are numerous PPI business models that allow the onboarding of third-party merchants with whom the value stored on the PPI may be redeemed. Such PPIs require authorization from the RBI before they are allowed to operate and are of the below five categories. The RBI has replaced the erstwhile classification of 'Semi-Closed' and 'Open' PPIs with 'Small' PPIs and 'Full KYC' PPIs.

The below five categories of PPIs are:

Si. No	Features	Small PPI (with cash loading)	Small PPI (without cash loading)	Full KYC	Gift Cards	Mass Transit System (MTS)
1.	Purpose	Only for purchase of goods and services at a group of identified merchants/ establishments		Can be used for purchase of goods and services (across multiple merchants), funds transfer or cash withdrawal.	Can be purchased by a person and redeemed by another person with a group of identified merchants/ establishments.	May be used at mass transit systems for fare collection, and merchant outlets whose activities carried on within premises of the MTS.
2.	KYC required / user details to be collected	Minimum details - mobile number (verified by OTP), self-declaration of name, identification number of any 'mandatory document' or another recognised official document. [107]		Authentication of the user to be completed as per RBI mandated regulations. [108]	Authentication of the purchaser to be completed as is done for Small PPI.	As decided by the Issuer.

107 As per the Master Direction on KYC: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566.

108 Id.

Si. No	Features	Small PPI (with cash loading)	Small PPI (without cash loading)	Full KYC	Gift Cards	Mass Transit System (MTS)
3.	Conversion	Shall be converted into full- KYC PPIs within 24 months from the date of issue, failing which, no further credits permitted.	N/A	N/A	N/A	N/A
4.	Reloadability	Shall be reloadable and issued only in electronic form. Can be reloaded via cash.	Shall be reloadable and issued in card or electronic form. Reloading to be done from bank account/ credit card/ full-KYC PPI. No reloading via cash	Shall be reloadable in nature and issued only in electronic form.	Not-reloadable	Reloadable
5.	Cash withdrawal / Funds transfer	Not allowed		Allowed For bank-issued PPIs: Subject to limit of INR 2000 (approx. USD 26) per transaction; Overall monthly limit of INR 10,000 (approx. USD 133) across all locations. For non-bank issued PPIs: Maximum of INR 2000 (approx. USD 26) per transaction within an overall monthly limit of INR 10,000 (approx. USD 133).	Not allowed	Not allowed

Si. No	Features	Small PPI (with cash loading)	Small PPI (without cash loading)	Full KYC	Gift Cards	Mass Transit System (MTS)
6.	Limits of funds transfer	N/A		In case of pre-registered beneficiaries, funds transfer limit shall not exceed INR 200,000 (approx. USD 2662) per month per beneficiary. For all other cases – limit is INR 10,000 per month (approx. USD 133).	N/A	N/A
7.	Monthly/yearly loading limits	Monthly – INR 10,000 (approx. USD 133). Yearly – INR 1,20,000 (approx. USD 1600)		No separate limit – PPI issuer may decide	Maximum value shall not exceed INR 10,000	No specified limit – PPI issuer may decide
8.	Outstanding amount limit	Shall not exceed INR 10,000 (approx. USD 133).		Shall not exceed INR 2,00,000 (approx. USD 2662)	N/A	Shall not exceed INR 3,000 (approx. USD 40)
9.	Closure of PPI	Allowed to close the PPI at any time; Closure proceeds can be transferred 'back to source account'		PPI issuer to give an option to close the PPI and transfer the balance as per the applicable limits	PPI may be revalidated (including through issuance of new instrument) when requested by PPI holder.	PPI may be revalidated (including through issuance of new instrument) when requested by PPI holder.
10.	Interoperability	Mandatory – see below for detail			Not mandatory - have the option to offer interoperability	Exempt from providing interoperability

Si. No	Features	Small PPI (with cash loading)	Small PPI (without cash loading)	Full KYC	Gift Cards	Mass Transit System (MTS)
11.	Additional Factor Authentication Required	All wallet transactions involving debit to the wallet, including cash withdrawal, shall be permitted only by validation through a Additional Factor Authentication (such as One-Time- Passwords or PINs). Through recent RBI circulars,[109] recurring payments up to an amount of INR 5,000 per transaction may be exempt from the AFA requirement subject to customer consent and preferences.			Not mandatory	Not mandatory
12.	Validity/ Redemption	PPIs issued in the country shall have a minimum validity period of one year from the date of last loading / reloading and can have a longer validity period as well. Non-bank PPI issuers cannot transfer the outstanding balance to their Profit & Loss account for at least three years from the expiry date of PPI. Refunds must be made in the event the PPI holder requests a refund after this three year period.				
13.	Maintenance of Logs	PPI issuers are to maintain a log of all the transactions undertaken using the PPIs for at least ten years, which must be made available for scrutiny to RBI or any other agency / agencies as may be advised by RBI.				

III. Eligibility for Authorization

Both banks and non-bank entities may apply for authorisation from the RBI to issue Small or Full KYC PPIs. Key points on the eligibility criteria to seek authorisation are as follows:

a. **Type of entity:** Non-bank entities applying for authorisation must be company incorporated in India and registered under the Companies Act, 1956 / 2013.[110] It would therefore not be possible for entities that are LLPs or sole proprietorships to apply.

b. **Charter Documents:** The Memorandum of Association (MoA) of the non-bank entity must cover the proposed activity of issuance of PPI.

c. **Net worth:** PPI issuers are required to have a minimum positive net worth[111] of INR 50,000,000 (approx. USD 680,000) at the time of submitting the application, with a requirement that PPI issuers must achieve a minimum positive net worth of INR 150,000,000 (approx. USD 2,040,000) by the end of the third financial year from the date of receiving final PPI authorization. This net worth is to be maintained at all times, and PPI issuers are required to submit their Net Worth Certificate (issued by a Chartered Accountant) every year.

109 https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11668; https://www.rbi.org.in/Scripts/NotificationUser.aspx? Id=12002; https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12051&Mode=0., (last accessed November 30, 2021).

110 Entities having Foreign Direct Investment (FDI) / Foreign Portfolio Investment (FPI) / Foreign Institutional Investment (FII) are required to meet the capital requirements as under the Consolidated FDI policy guidelines of Government of India.

111 2.7 Net-worth : Shall consist of 'paid up equity capital, preference shares which are compulsorily convertible into equity capital, free reserves, balance in share premium account and capital reserves representing surplus arising out of sale proceeds of assets but not reserves created by revaluation of assets' adjusted for 'accumulated loss balance, book value of intangible assets and deferred revenue expenditure, if any'. While compulsorily convertible preference shares reckoned for computation of net-worth can be either non-cumulative or cumulative, these shall be compulsorily convertible into equity shares and the shareholder agreements shall specifically prohibit any withdrawal of this preference share capital at any time.

IV. Application and Authorization Process

a. **Application Process:** Applicants must apply for authorization by submitting Form A[112] to the RBI. Once Form A has been submitted and if the RBI finds that the applicant has met the eligibility criteria, they shall issue an "in principal" approval, which is valid for 6 months, which may be extended for a year at the discretion of the RBI. The applicant would then be required to submit a satisfactory System Audit Report (SAR) and a net worth certificate of INR 5 crore within these six months. Once this is submitted, RBI may then grant a final certificate of authorization, which maybe for a perpetual period, subject to meeting certain conditions,[113] as was clarified in a circular issued in December 2020[114].

b. **Introduction of a Cooling Period to Ensure 'Serious Applicants':** As was clarified in a circular issued in December 2020,[115] the there is a cooling period of one year before the following entities may re-apply for PPI authorization:

   - PPI issuer whose Certificate of Authorization **("CoA")** is revoked or not-renewed for any reason; or
   - CoA is voluntarily surrendered for any reason; or
   - Application for authorization has been rejected by RBI; or
   - New entities that are set-up by promoters involved in any of the above categories.

c. **Financial regulator NOC:** Both banks and non-banks regulated by any "financial sector regulator" and seeking authorization under the Master Direction must submit a No Objection Certificate (NOC) from their respective regulator as part of the application for authorization.

d. **'Fit and proper' status:** The RBI has extended the fit and proper criteria (which typically applies to banks and NBFCs) to entities applying for authorization under the Master Direction. Further, directors of the applicant are required to submit an undertaking.

e. **Changes in Products/Features/Change of Control:** The PPI Regulations mandate that any proposed major change, such as changes in product features / process, structure or operation of the payment system, etc., as well as any takeover or acquisition of control or change in management of a non-bank entity is to be communicated to the RBI within 15 days of such change taking place.

   In the past, there have been conflicts as the 2017 Regulations had a reporting requirement, while the terms and conditions of the PPI Authorisation had provided for an authorisation to be sought for the above changes. Hence, going forward, this point should be clarified in the PPI authorisation terms and conditions for consistency.

V. Co-branding

In the event an entity does not wish to seek RBI authorization itself, the PPI Regulations allow entities to co-brand with existing PPI Issuers in order to issue PPIs. In such instances, companies incorporated in India (which may also be a Government department / ministry) are allowed to co-brand with existing PPI Issuers. The PPI Regulations prescribe certain conditions for co-branding on the PPI Issuer, which include

112 https://rbidocs.rbi.org.in/rdocs/Forms/PDFs/PSSACRT130215.PDF, (last accessed November 30, 2021).

113 Full compliance with the terms and conditions subject to which authorisation was granted; Fulfilment of entry norms such as capital, net worth requirements, etc.; No major regulatory or supervisory concerns related to operations of the PSO, as observed during onsite and / or offsite monitoring; Efficacy of customer grievance redressal mechanism; and no adverse reports from other departments of RBI / regulators / statutory bodies, etc.

114 https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12000&Mode=0, (last accessed November 30, 2021).

115 https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12001&Mode=0, (last accessed November 30, 2021).

having a board approved policy that allows for such co-branding, and conducting due diligence and KYC, to name a few.

Additionally, the PPI Issuer is to be liable for all acts of the co-branding partner, and will be responsible for all customer related aspects of the PPI. Whilst a one-time approval is still required for PPI Issuers to issue co-branded PPIs, the erstwhile requirement under the 2017 Regulations to report specific co-branding arrangements to the RBI has been done away with.

VI. Customer Protection / Grievance Redressal

A few key conditions under the PPI Regulations are that:

a. PPI Issuers are required to disclose all important terms and conditions in clear and simple language (preferably in English, Hindi and the local language) to the holders while issuing the instruments. The Frequently Asked Questions (FAQs) pertaining to PPIs are to be displayed on the PPI Issuer's website/ application.

b. A formal, publicly disclosed customer grievance redressal framework is to be put in place.

c. PPI issuers are to clearly indicate the customer care contact details, including details of nodal officials for grievance redressal (telephone numbers, email address, postal address, etc.). Further, a detailed list of the PPI Issuer's authorised / designated agents is also to be displayed.

d. PPI Issuers are expected to initiate action to resolve customer complaints preferably within 48 hours and endeavour to resolve such complaints no later than 30 days from the receipt of the complaint.

VII. Interoperability

The 2017 Regulations had mandated that interoperability (the ability to use one payment system with another) would be implemented in phases, and that operational guidelines on interoperability would be issued. An RBI Circular issued in May 2021 [116] subsequently mandated that KYC compliant PPIs were to ensure interoperability, while PPIs for mass transit systems and gift cards are exempted. This involves interoperability of PPIs issued via wallets and card networks, PPIs issued via card networks, and PPIs issued via UPI. Technical and operational requirements have been issued in this regard.

VIII. Co-mingling of funds

Settlement of funds with merchants shall not be co-mingled with other businesses, if any, handled by the PPI issuer, or with any other activity that they may be undertaking such as Business Correspondents of bank/s, intermediary for payment aggregation, payment gateway, etc.

116 https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12094&Mode=0, (last accessed November 30, 2021).

IX. Cross border transactions

Use of INR dominated PPIs for cross border transactions is not permitted, except in the below instances:

a. Cross border outward transactions[117] via Full KYC PPIs issued by authorized dealer banks, subject to foreign exchange laws. This feature may be enabled only on explicit request of the PPI holder and will be subject to transaction limits, i.e. not exceeding INR 10,000 per transaction, and INR 50,000 per month. Such PPIs shall not be used for cross border outward fund transfers or payments under the Liberalized Remittances Scheme (LRS).[118] Further, such PPIs cannot be issued by non-banks.

b. Cross border inward transactions via Full KYC PPIs issued by both banks and non-banks appointed as Indian agent of authorized overseas principals to beneficiaries of inward remittances under the Money Transfer Services Scheme (MTSS) of RBI. This is subject to certain conditions as prescribed under the PPI Regulations.

X. Settlement/Escrow Account

Non-bank PPI issuers are to process settlements only through sponsor banks, and are required to maintain outstanding balances in an escrow account with scheduled commercial banks.

XI. Outsourcing Considerations

The RBI has also released regulations for the outsourcing of payment and settlement-related activities to third party service providers non-bank payment system operators / providers, which include PPI Issuers. Hence, entities not directly regulated by the RBI may be subject to certain contractual compliances and restrictions imposed by payment system operators as part of the latter discharging their legal obligations. You may read more about this development here[119].

XII. Customer Protection Guidelines

PPI Issuers must also follow certain RBI Guidelines on limiting liability of customers in unauthorized electronic banking transactions. These guidelines prescribe obligations such as reporting of unauthorized payment transactions to customer, and limiting customer liability in certain instances.

Conclusion – Need For Further Liberalization

The compilation of the various circulars released by the RBI on PPIs through the years, as well as the clarity on Closed System PPIs, opening up the offering of PPIs permitting cash-based withdrawal to non-bank PPI Issuers, and the detail on Interoperability are a welcome change to the industry. The mandate on all debits to PPI instruments requiring AFA, however, may see a mixed reaction as this would take away from the convenience that PPIs offer customers.

117 For permissible current account transactions under FEMA, i.e. for purchase of goods of services.

118 Further, prefunding of online merchant's account shall not be permitted using such Rupee denominated PPIs.

119 https://www.nishithdesai.com/NewsDetails/4796 (last accessed November 30, 2021).

A few suggestions to further liberalize the regime are as follows:

Taking a leaf out of UPI's book, RBI could consider opening up cross border transactions to boost market entry and ease of doing business for foreign players.

The high net worth requirements continue to be a barrier to market entry, which would explain why there are barely any new players who enter the space. Entities who do not wish to come up with these high net worth requirements often turn to co-branding or white labeling arrangements.

When it comes to co-branding requirements, the PPI Regulations still do not allow foreign entities to co-brand with PPI Issuers, which is an unnecessary hurdle for offshore players.

The mandatory requirement to 'convert' cash-loading Small PPIs to Full KYC PPIs within 24 months from the date of issue, may lead to pressure on issuers to alter their business models to provide PPI holders with added features. It should be clarified whether the requirement is for cash-loading Small PPIs to merely complete the KYC within 24 months, or whether to convert the instrument to the nature of a 'Full KYC' PPI as envisaged under the PPI Regulations, which can also be used for funds transfer and cash withdrawal.

Overall, while it is acknowledged that there has been limited liberalization of the PPI regime via exempting recurring payments, and extending the authorization for a perpetual period, further steps towards liberalization would be appreciated by the industry to revive the growth of PPIs in India, especially when compared to the tremendous growth and volumes of UPI, mobile banking and 'buy-now-pay-later' payments.

— Inika Charles, Aaron Kamath & Huzefa Tavawalla

November 24, 2021

K. View: Two tremendous transitions too soon for Digital Payments Industry

Click the above logo to visit the published article

Industry players need a breather post recurring payments revamp

The Reserve Bank of India (RBI) has with effect from October this year completely revamped the regime for online automatic payments, leaving online merchants gasping. Payment aggregators and online merchants now need to brace for another potentially disruptive transition from January 1, 2022. Effective from the new year, payment aggregators and online merchants cannot store card and certain payment data, as a result of RBI's concerns around alleged data leaks in the fintech space involving volumes of card information. RBI provided tokenization of card data as an alternate solution. A balanced approach is needed to consider the interests of all stakeholders viz. consumers, e-commerce merchants and fintech players. Given that extensive technological, operational and integrational aspects need to be developed, tested and deployed in the payments ecosystem, RBI should consider a transitional timeline of at least 6–12 months for solutions such as tokenization to be implemented.

Healing from the automatic payments wound

Many of you would have received multiple communications from your banks in September informing you that your online subscription automatic payments may be discontinued from October 1, 2021 and would need to be re-registered. This was because back in September 2019, the RBI introduced an entirely new regime to register online automatic payments. The new regime required banks not to permit recurring payments unless the e-mandates are registered in under the new regime.

On the face of it, two years seemed a liberal timeline for implementation of the new regime, though the reality is that reportedly, over 70% of standing instructions failed on October 1, 2021 and many continue to fail.[120] This is primarily because banks did not implement requisite infrastructure on a timely basis, as they were not legally mandated to by the RBI. Those affected were consumers whose subscriptions payments were not only interrupted but many of which were not able to re-register under the new regime.

This led to users having to manually effect payments reducing payment success rates leading to loss of revenues for merchants.

120 https://www.livemint.com/industry/banking/why-payment-policies-have-triggered-chaos-11635786988391.html, accessed on Nov 15, 2021.

New conundrum to tackle on new years' day

Under a separate set of directives regulating payment aggregators, the RBI has prescribed that effective from January 1, 2022 neither payment aggregators nor online merchants can store customer card and related data. The RBI in March this year further clarified that merchants cannot 'payment data' without defining or clarifying the meaning of such a term and the items of data included with its scope.

Tokenization the talk of the town

Storage restrictions will require users to fill in their card or other payment instrument details for every online transaction. Manual filling of payment instrument details would be required for each online transaction affecting payment latency rates, user experience, continuity of customer service and revenues of online merchants. Furthermore, auto-recurring payments would not be possible. This would disrupt online services that consumers have subscribed to leading to inconvenience, whether the services are for consumers' personal enjoyment or earning personal livelihood, examples include domain registrations, web-hosting services etc.

To remedy this inconvenience, card-on-file (CoF) tokenization can be considered, which entails a token which is device-independent and consists of the card, token requestor and merchant details. The process essentially involves the storage of 'tokens' that do not consist of, contain or identify any of the users' payment or card data, but corresponds to the payment instrument of a user. However, the tokenization process comes with its own set of challenges.

Patience is key to efficiency

Tokenization is a process which involves multiple stakeholders including the merchant, token requestor, payment aggregator, token service provider, card network and banks and in some cases technology infrastructure or services providers. While the RBI imposed restrictions on data storage in March 2020, the CoF tokenization was permitted by the RBI only in September 2021. Stakeholders essentially have only 3 months to design, implement and test viable infrastructure, which isn't remotely enough. One weak link will cripple the entire infrastructure.

It is understood from industry players that even if banks are ready with their technology integrations, merchants would need at *least 6 months* to integrate their systems for CoF tokenization. This additional time is important for merchants to conduct necessary testing on the new infrastructure for robust system functionality, security and performance.

Operational hurdles

Additionally, certain operational challenges need to be ironed out.

- One issue pertains to the requirement of purging existing data, which may lead to issues in the merchant initiating refunds, redressing complaints and offering rewards or incentives to users that have not been able to register their payment instrument details via tokenization. RBI should prescribe a transitional timeline for purging of card data for merchants' business continuity purposes and to prevent service disruption to consumers.

- Secondly, tokenization of a user's payment instrument requires their consent and additional validation, and the same process is required for a replaced or renewed instrument. This appears onerous since a user who receives a new card replacing their expired or lost card, would need to re-register the new card even though the new card has the same cardholder details and is linked to the same bank account and customer ID. RBI should consider a relaxation in re-tokenizing renewed/replaced cards linked to the same user account.
- Thirdly, RBI clarified that the last four digits of the card and cardholders name can continue to be stored for transaction tracking and reconciliation purposes. However, the first four or six digits that identify the bank (BIN) are also required to be stored in order to identify the issuer. The RBI should permit BINs to be stored, at least for security, tracking and reconciliation purposes.
- Fourthly, banks that have needed frequent nudges from the RBI and industry players in the past, should be mandated to implement the requisite infrastructure for enable tokenization.

The industry awaits much-needed clarifications from the RBI which could be issued in the FAQs, as done in the past.

— Gowree Gokhale, Huzefa Tavawalla and Aaron Kamath

August 19, 2021

L. First of its kind outsourcing regulatory framework for payment service providers

Background

The Reserve Bank of India **("RBI")**, India's apex bank recently issued a regulatory framework **("Framework")** to be implemented by non-bank payment system operators / providers **("PSPs")** for the outsourcing of payment and settlement-related activities to third party service providers. PSPs have been provided with a timeline of until March 31, 2022 to ensure that their outsourcing arrangements comply with the Framework.

What is a PSP?

As per the Payment and Settlement Systems Act, 2007 **("PSS Act")**, a "payment system" means a *"system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlementservice or all of them, but does not include a stock exchange".*[121] Payment systems include systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations. An entity that operates a payment system is considered a 'payment system operator' (PSO) or 'payment system provider' (PSP), which needs to be authorized by the RBI. PSPs can include payment aggregators, e-wallet and gift instrument issuers, card issuers and networks, money transfer networks, ATM networks and National Payments Corporation of India (NPCI) that operates the Unified Payments Interface (UPI), a system for fund transfers between bank accounts via a mobile platform.

Scope of The Framework

'Outsourcing' under the Framework means use of a third-party service provider to perform activities on a continuing basis that would normally be undertaken by the PSP. 'Service providers' include vendors, payment gateways (PGs), agents, consultants and their representatives engaged in payment and settlement systems activities, including subcontractors or secondary service providers.

The Framework seeks to put in place minimum standards to manage risks involved in outsourcing of payment and settlement-related activities by PSPs, including incidental activities like on-boarding customers, IT services etc.[122] The Framework is applicable to outsourcing of functions by PSPs to service providers in India and overseas.

Outsourcing Functions

The PSP should ensure that it exercises due diligence, implements appropriate risk management practices for oversight, and manages risks arising from the outsourcing of activities. Specifically, in terms of critical processes and activities, the Framework requires PSPs to first evaluate the need to outsource such functions based on a comprehensive risk assessment.

121 Section 2(i) of the PSS Act.

122 Though is not applicable to activities not relating to payment / settlement services, such as internal administration, housekeeping orsimilar activities.

The outsourcing should not impede or interfere with the ability of the PSP to oversee and manage its activities, nor prevent the RBI from carrying out its supervisory functions. More importantly, the PSP shall continue to be held liable for the actions of its service providers.

Outsourcing Restrictions

The Framework restricts PSPs from outsourcing 'core management functions' that include risk management, internal audit, compliance and decision-making functions such as determining KYC compliance. 'Core management functions' include management of the payment system operations, transaction management, according sanction to merchants for acquiring, managing customer data, risk management, information technology and information security management.

PSP Compliance Framework

The Framework sets out a host of compliance obligations to be fulfilled by the PSP in outsourcing functions to service providers, broadly including the following:

1. **Supervisory Functions:** The PSP would be responsible for the outsourced activity and liable for the actions of its service providers; hence it should retain ultimate control over the outsourced activity.
    a. PSPs should consider all relevant laws, regulations and conditions of regulatory authorization or licenses when outsourcing functions,
    b. Rights of a customer and a participant of payment system against a PSP should not be affected, including
    c. grievance redressal,
    d. If the PSP has outsourced its customer grievance redressal function, it should provide its customer the option of direct access to its nodal officers for raising or escalating complaints, and
    e. In cases wherein the customer has an interface with the service provider, the PSP should clearly indicate to the customer the role of the service provider.
2. **Governance:** PSPs should have in place a board-approved comprehensive outsourcing policy setting out amongst other things, criteria for selection of outsourcing activities and service providers, parameters for grading the criticality of outsourcing; delegation of authority depending on risks and criticality; and systems to monitor and review the operation of these activities. In addition,
    a. The Framework sets out the role of the board of the PSP in relation to outsourcing, such as deciding on business activities to be outsourced and approving a framework to evaluate risks and criticality involved in outsourcing.
    b. The Framework further confers responsibilities on senior management of the PSP in relation to evaluating risks and criticality associated with outsourcing functions, ensuring contingency plans are in place and periodically tested and ensuring an independent review and audit for compliance.
    c. All outsourcing arrangements should be maintained in a central record of the PSP, updated and reviewedperiodically, and readily accessible to the board and senior management.
    d. The PSP should ensure that the service provider has a robust framework for documenting, maintaining and testing business continuity and recovery procedures arising out of outsourced activities, which should bereviewed and tested periodically by the service provider.

e. The PSP should consider availability of alternative service providers, and the prospect of bringing back theoutsourced activity in-house in case of an emergency.

Furthermore, the Framework restricts a director or officer or their relatives of a PSP in owning or controlling another service provider, unless it is a group company of the PSP.

3. **Outsourcing agreements:** The Framework provides certain requirements for the terms and conditions governing the PSP and their service provider. It should be in writing, reviewed by PSP's legal counsel and address risks and strategies for mitigating risks. The agreement should allow the PSP to retain adequate control over the outsourced activity and the right to intervene when necessary for compliance with law.

Key provisions of the outsourcing agreement should include:

a. Defining the activity to be outsourced including service standards,

b. PSP's access to all books, records and information available with the service provider relevant to the outsourced activity,

c. PSP's continuous monitoring and assessment of the service provider,

d. Termination clause and minimum period to execute such provision, if necessary,

e. Service provider's obligation to ensure controls are in place for maintaining confidentiality of customer data,

f. Service provider's liability in case of breach of security and leakage of customer information,

g. Contingency plans to ensure business continuity,

h. Requirement of PSP's prior approval in case of sub-contracting arrangements,

i. PSP's audit rights over the service provider,

j. RBI or RBI authorized persons to access PSP's documents, transaction records and other information stored or processed by the service provider,

k. RBI's right to inspect the service provider and their books of accounts,

l. Service provider's obligations to comply with RBI directions involving activities of the PSP,

m. Service provider's obligation to maintain confidentiality of customer information post expiry or termination of the agreement,

n. Preservation of documents and data by the service provider and protection of PSP's interests post termination of the outsourcing arrangement.

4. **Confidentiality and Security:** PSP's should ensure that the service provider maintains security and confidentiality of customer information in their custody or possession.

a. Access to the service provider's staff should be limited and on a 'need to know' basis,

b. The service provider should not co-mingle and should be able to isolate and identify the PSP's customerinformation, documents, records and assets to protect confidentiality,

c. The PSP should regularly review and monitor the security practices and control processed of the service provider,

d. The service provider should report security breaches to the PSP,

e. The PSP should report to the RBI any security breaches and customer confidential information leakages. Liability to customers for such breaches would lie with the PSP.

f. PSPs should ensure that the service provider, whether domestic or offshore, adheres to the RBI's instructions on storage of payment system data.

Outsourcing Within Group/Conglomerate Entities

The Framework specifically address PSP's having service arrangements with group entities; for instance, legal and professional services, IT applications, back-office functions, outsourcing payment and settlement services etc. Such arrangements should be based on the PSP's board approved policy and service level arrangements with its group entities.

PSP's should ensure that:

1. The agreements cover demarcation of shared resources like premises, personnel etc.,
2. In case of multiple group entities cross-selling, customers should be informed about the actual entity offering the product or service,
3. The agreements should be in writing and cover details like scope of services, charges and confidentiality of customer data,
4. The arrangement should not cause confusion among customers, as to whose products or services they are availing, by clear physical demarcation of the site of activities of different group entities,
5. The arrangements should not compromise the ability of the PSP to identify and manage risks on a standalone basis,
6. The arrangements should not prevent RBI from obtaining information required for supervision of the PSP or to the group as a whole,
7. The PSP's ability to carry out operations in a sound fashion is not affected if premises or other services like IT or support staff services provided by the group entity are interrupted,
8. Risk management practices adopted by PSP's for outsourcing to group entities should be the same as prescribed in the Framework for a non-related party.

Outsourcing To Overseas Entities

The PSP should monitor Government policies, political, social, economic and legal conditions in countries where the service provider is based, both during the risk assessment process and on a continuous basis. Contingency and exit strategies should be in place.

In outsourcing services relating to Indian operations to offshore entities, the PSP should ensure that:

1. In principle, arrangements should be with parties in jurisdictions that generally uphold confidentiality clauses and agreements,
2. The governing law of the agreement is clearly specified,
3. The activities outsourced should be conducted in a manner to not hinder efforts to supervise or reconstruct the India activities of the PSP,
4. The offshore regulator should not obstruct to the arrangement nor object to RBI's visits for audit, scrutiny, examination, inspection, assessment or visits from PSP's internal and external auditors,

5. The offshore regulator does not have access to the data relating to the PSP's India operations, and
6. The jurisdiction of courts in the offshore jurisdiction does not extend to the PSP's operations in India merely because data is processed in the offshore location.

Participants in the Payments Ecosystem

The PSP should also engage with all participants in a payment transaction to *encourage* them to implement the Framework. Specifically, in respect of payment systems operated by PSPs involving other participants such as token requestors in tokenization solutions, third-party application providers in UPI systems etc. who may not be directly regulated or supervised by RBI; but it is prudent for such participants to put in place systems to manage risks arising out of activities outsourced by them.

The above provisions from the Framework do not appear to relate per se to outsourcing activities, though appear to suggest that non-licensed entities in the payment's ecosystem are encouraged to adopt appropriate security and risk mitigation measures.

Analysis

Firstly, payment intermediaries were historically not directly regulated by the RBI but instead since 2009, were indirectly via AD banks with whom they needed to have nodal accounts for settlement of transactions between merchants and consumers. In a paradigm shift since March 2020, payment intermediaries that handle the funds, in receiving, pooling and transferring funds from customers to merchants were directly regulated and put under a licensing regime by the RBI. This was the first step to regulating payment aggregators, a type of a PSP.

However, certain other PSPs were and continue to be regulated under the PSS Act and RBI regulations, for instance, e-wallet and gift instrument issuers. In fact, PSPs are being drawn a wider net of regulation in recent years, given the important role that they play in payment transactions, for instance imposition of data localization norms. Having said that, *outsourcing functions of PSPs* were not previously regulated, unlike in the case of banking and non-banking financial companies (NBFCs) wherein specific RBI directives were issued on the subject. Hence, this is a first of its kind regulation for outsourcing functions of PSPs.

Secondly, the Framework doesn't substantially differ from the previous RBI directives on outsourcing applicable to banks and NBFCs which also contained provisions along the same lines such as control and supervision, risk assessments and policies, confidentiality and security, outsourcing agreements, outsourcing restrictions, grievance redressal and outsourcing within group entities / conglomerates, and to offshore service providers. Hence, whilst the Framework is a first for PSPs, it appears to only follow precedent that the RBI has set in regulating outsourcing functions by regulated entities, though more sophisticated. This entails that PSPs would follow the route taken by banks and NBFCs in terms of governance and contractual compliances when outsourcing functions to service providers.

Thirdly, the Framework restricts outsourcing of 'core management functions', which includes some of the obvious functions meant to be carried out directly by the PSP such as management of payment system operations, transactions and risk management, audits, compliance and decision-making functions. However, managing customer data and IT and InfoSec management is also considered a 'core management function' that cannot be outsourced. Further, customer data is defined to include payments-related data / information.

Basis this and considering the recent data storage restrictions, it will be interesting to see how the industry views "management" especially in the context where data storage / processing functions are outsourced but the PSP continues to retain overall control / rights over the data. In such situations it would need to be evaluated whether the same would be viewed as outsourcing of a core management function.

Similarly, it is common for banks, NBFCs and even PSPs to engage service providers for IT and InfoSec services and to provide systems and solutions for the former's business operations. Such arrangements would also need to be evaluated to determine whether it constitutes outsourcing of 'management' functions.

Also, the Framework identifies 'core management functions' in a non-exhaustive manner by using the term "including". Thus, unless clarified by the RBI, it would always be subjective and open to interpretation on what other functions would be deemed to be 'core management functions' which should not be outsourced by PSPs.

Finally, from a cross-border perspective, PSPs would need to evaluate existing and future arrangements keeping in mind additional requirements. Requirements for the PSP to ensure that the offshore regulator does not object to RBI/PSP's visits and audits and does not access the data to the PSP's India operations and offshore Courts' jurisdiction does not extend to PSP's operations in India; go beyond the offshore outsourcing provisions applicable to banks and NBFCs. PSPs would need to implement extra steps and assessments which may include understanding and taking legal opinions on applicable foreign laws prior to entering into such offshore outsourcing arrangements, as well as tailor the outsourcing agreements to address the cross-border requirements.

Conclusion

From a user perspective, this Framework is a welcome step where non-bank PSPs would be subject to outsourcing compliances which would largely benefit consumer interest. This is also in line with the existing outsourcing regulations as applicable to banking and non-banking financial companies. However, given the advancements in technology and security solutions along with business prowess of new fintech players including PSPs, outsourcing certain activities relating to managing customer data, IT services and InfoSec functions should be permitted subject to relevant compliances under the Framework.

Consumer interests could still be protected as PSPs would need to comply with the Framework including implementation of risk evaluation policies, security standards, audits, controls and stringent contractual arrangements with third party service providers. Thus, categorizing the said activities as 'core management functions' which cannot be outsourced may impact the growth and innovation of the industry.

— Aaron Kamath & Huzefa Tavawalla

March 24, 2020

M. Licensing Regime Introduced For Payment Aggregators: E-Commerce Industry to Undergo Significant Change

The Reserve Bank of India **("RBI")**, India's central and apex bank on March 17, 2020 issued detailed guidelines[123] **("Guidelines")** applicable to payment aggregators **("PAs")**, which shall come into effect from April 1, 2020.

Going forward PAs will need to an authorization / license to operate from the RBI. No authorization /license is prescribed for payment gateways **("PGs")**. While Guidelines recommend certain good practices for PGs, they are not mandatory. Since 2009, RBI regulated entities who were facilitating payments between users and merchants using any electronic / online payment mode, via intermediary directions dated November 24, 2009[124] **("Intermediary Directions")**.

The RBI had earlier in September last year floated a discussion paper[125] **("Discussion Paper")** wherein it was exploring regulating PAs and PGs, given that they form a critical link in the online world of commerce. Some key concerns raised by the RBI in the Discussion Paper were:

i. The activities of PAs and PGs in online transactions are extremely crucial and such entities may be a source of risk, if they have inadequate governance practices that may impact customer confidence and experience.

ii. A customer has very limited recourse to PAs and PGs and must rely on merchants or banks who in turn seek redressal from the PAs.

iii. Being part of the payments process chain, these entities also handle sensitive customer data. Hence, managing customer data, data privacy and know-your-customer (KYC) requirements of merchants are important from a security and customer confidence perspective.

Basis the above, it appears that the Discussion Paper paved the way for the said Guidelines. For ease of reference, we have sought to break down the Guidelines in a Q&A format as detailed below.

What are PAs and PGs?

The Guidelines define 'payment aggregators' as *"entities that facilitate e-commerce sites and merchants to accept various payment instruments from the customers for completion of their payment obligations without the need for merchants to create a separate payment integration system of their own. PAs facilitate merchants to connect with acquirers. In the process, they receive payments from customers, pool and transfer them on to the merchants after a time period."* Thus, PAs are those entities that facilitate payments to merchants, and that receive, pool and transfer user payments to the merchants as part of the facilitation process.

On the other hand, 'payment gateways' are defined as *"entities that provide technology infrastructure to route and facilitate processing of an online payment transaction without any involvement in handling of funds."*

123 Available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0, Last accessed: March 19, 2020.

124 Available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=5379&Mode=0, Last accessed: March 19, 2020.

125 Available at: https://m.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=943, Last accessed: March 19, 2020.

Thus, PGs under the Guidelines may be limited to entities providing authentication services, back-end infrastructure or technology integrations services which assist in the payment ecosystem.

However, this understanding would need to be further examined basis the existing law on intermediaries (as discussed in the below Q&A).

Who does the Guidelines Extend to?

The Guidelines are specifically applicable to PAs, though there are also recommended good practices (non-binding) for PGs, such as security and data retention related measures. The Guidelines even apply to domestic legs of import and export related payments facilitated by PAs.

The Guidelines do not apply to cash-on-delivery e-commerce models.

When do the Guidelines Become Effective?

Any new entity that intends to offer the services of a PA post April 1, 2020, would be subject to the said Guidelines. Thus, with effect from April 1, 2020 any new entity intending to provide PA services can only do so post authorization from the RBI.

For existing PAs, they need to apply for RBI authorization on or before June 30, 2021 and then they would be allowed to continue operations until they hear back from the RBI on their application. However, it appears unclear from the Guidelines that until such authorization has been obtained by existing PAs, whether such PAs would continue operating as per the Intermediary Directions or adopt measures and compliances under the Guidelines.

This is an aspect that requires further clarity from the regulators.

What is the Inter Play Between PAs and Intermediaries?

As per the Intermediary Directions, intermediaries were defined as: *"all entities that collect monies received from customers for payment to merchants using any electronic/online payment mode, for goods and services availed by them and subsequently facilitate the transfer of these monies to the merchants in final settlement of the obligations of the paying customers."*

The said Intermediary Directions also stipulated compliances involving use of nodal accounts, permissible debits / credits in such nodal accounts, time periods for final settlement of funds to merchants etc. However, as per the said Intermediary Directions, entities operating as intermediaries were not required to obtain an authorization / license from the RBI for undertaking the said activities.

On the other hand, PAs under the said Guidelines appear to be a sub-set of an intermediary as they also facilitate transactions between users and merchants by pooling funds and transferring them to merchants. Thus, the question which arises is would there be any intermediaries (as per the Intermediary Directions) which would not be categorized as PAs under the said Guidelines, and if so, how would such intermediaries continue to be treated. Going by the intent, it seems that the Intermediary Directions would be phased out once the Guidelines are fully into effect.

What are the Key Eligibility Criteria for a PA to obtain RBI Authorization?

i. **Authorization:** Bank PAs do not need separate authorization from RBI. Non-bank PAs are required to seek an authorization from RBI. Only a company (as opposed to other types of entities) is eligible to register as a non-bank PA. An LLP would not be eligible for such RBI authorization.

ii. **Marketplaces:** E-commerce marketplaces providing PA services cannot continue the said activity beyond June 30, 2021. If they desire to do so, the PA services will have to be separated from the market-place business and then an application for authorization as a PA will need to be made on or before June 30, 2021. Such internal restructuring could lead to significant tax & contractual issues which will need to be evaluated on a case to case basis.

iii. **Capital Requirements:** Existing PAs are to have a net-worth of INR 15,00,00,000 (approx. USD 2,000,000) by March 31, 2021 and net-worth of INR 25,00,00,00 (approx. USD 3,330,000) by the end of the 3rd financial year, i.e. on or before March 31, 2023. This net-worth should be maintained at all times thereafter. New PAs should have a minimum net-worth of INR 15,00,00,000 (approx. USD 2,000,000) at the time of filing its application for RBI authorization and should attain a net-worth of INR 25,00,00,000 (approx. USD 3,330,000) by the end of the 3rd financial year from the grant of authorization. This net-worth should be maintained at all times thereafter.

What is the Role that PAs Will Play in Settlement of Transactions Going Forward?

Unlike as prescribed under the Intermediary Directions wherein intermediaries are required to open a nodal account, the Guidelines prescribe that a non-bank PA maintain an escrow account with any one scheduled commercial bank for amounts collected, which the PA may also pre-fund. The escrow account cannot be used for or co-mingled with other businesses, if any, of the PA. The amounts held in the escrow account should be interest free, except under certain circumstances as maybe determined between the PA and bank.Once the amount is deducted from a user's account, it should be remitted to the escrow account on a 'T'+0 or 'T'+1 basis. Thereafter, final settlement with the merchant may take place as follows:

- If the PA is responsible for the delivery of goods / services – 'T'+1 basis wherein T is the date of intimation by the merchant to the intermediary about the shipment of goods.
- If the merchant is responsible for delivery – 'T'+1 basis wherein T is the date of confirmation by the merchant to the PA about the delivery of goods
- If the agreement provides for the PA to keep the amount till expiry of refund period – 'T'+1 basis where T is the date of expiry of the refund period fixed by the merchant.

The escrow account should also be used to route credits towards reversed transactions and refunds.

Similar to that of a nodal account, the escrow account to be opened by PAs allows for only certain credits and debits,as follows:

Credits

a. Payment from various customers towards purchase of goods / services.

b. Pre-funding by merchants / PAs.

c. Transfer representing refunds for failed / disputed / returned / cancelled transactions.

d. Payment received for onward transfer to merchants under promotional activities, incentives, cash-backs etc.

Debits

a. Payment to various merchants / service providers.

b. Payment to any other account on specific directions from the merchant.

c. Transfer representing refunds for failed / disputed transactions.

d. Payment of commission to the intermediaries. This amount shall be at pre-determined rates / frequency.

e. Payment of amount received under promotional activities, incentives, cash-backs, etc.

What are the Key Compliances Applicable to PAs?

i. **Technology** – The PA should have a board approved policy for information security for the safety and security of the payment systems operated and such measures should be implemented. A PA should put in place adequate information and data security infrastructure and systems to prevent and detect fraud, and other technology based recommendations as provided in the Guidelines.

ii. **Governance** – The promoters of the PA entity should satisfy a 'fit and proper' criteria prescribed by the RBI and the directors are to submit an undertaking as per the prescribed format. A PA should have a board approved policy for disposal of complaints / dispute resolution mechanism and time-lines for processing refunds etc. as per timelines prescribed by the RBI. A nodal officer should also be designated for regulatory functions and to handle customer complaints as well as an escalation matrix.

In terms of documentation, a PA should have (i) agreements in place with merchants, acquiring banks and other stakeholders that delineate the roles and responsibilities of each party in handling complaints, refunds, returns, customer grievances, dispute resolution and reconciliation, and (ii) disclosure comprehensive information regarding merchant policies, customer grievances, privacy policy and other terms and conditions on its website / application.

Furthermore, any takeover or acquisition of control of change in management of a non-bank PA should becommunicated to the RBI within 15 days. Although not explicit, it appears that this reporting requirement triggers post the corporate action taking place. However, given the ambiguity, it may be preferable to notify the RBI prior to such corporate action, given that the Guidelines give discretion to RBI to place restrictions on such changes, if deemed suitable.

iii. **Merchant on-boarding** – A PA should have a board approved policy for merchant on-boarding. In addition, the PA should conduct background and antecedent checks on the merchant to ensure that they do not have a history of duping customers or selling fake / counterfeit / prohibited products.

iv. **KYC** – The Guidelines also make prevailing KYC norms applicable to PAs. Though unclear, it appears that PAs and PGs should conduct KYC checks on its customers, which may be merchants and / or end users, basis the nature of each arrangement.

Generally, this KYC requirement should apply only to PAs vis-à-vis the merchants since the merchants are considered customers of the PA and have a direct contractual arrangement with such PAs. However, further clarity on the same by the RBI would be helpful.

v. **Security and Data** – The Guidelines also prescribe certain security, fraud prevention and risk management compliances for PAs, in terms of policies to adopt and measures to implement. Specifically, PAs should not store customer card credentials on their systems that may be accessed by the merchant. PA's would also be subject to the data storage requirements applicable to payment system operators, which appear to also include data localization requirements in terms of end-to-end transaction data.[126] Hence, such data would not be able to be transferred outside India, unless in certain circumstances and subject to certain compliances.

   There is also a requirement for PAs to take preventive measures to ensure that data is stored in 'infrastructure that does not belong to external jurisdictions'. This requirement of data sovereignty appears vague and unclear. Situations where an Indian company (which is a wholly owned subsidiary of a foreign company) or any other Indian owned / controlled entity using foreign technology to provide data storage services to PAs would need to evaluate whether they fulfil the necessary data compliance requirements.

Conclusion

It appears that many of the prescribed compliances as per the Guidelines are similar to those already prescribed by the RBI for payment system operators, such as e-wallet and gift card issuers, and it appears that the RBI is placing PAs on the same pedestal as such payment system providers in terms of regulation.

Also, the obligations placed on PAs vis-à-vis merchants such as conducting background checks on the merchant's history to ensure that they do not have a history of duping customers or selling fake / counterfeit / prohibited products, appears onerous and practically difficult to implement. Although one could consider evaluating self-declarations made by merchants in this regard.

These Guidelines also bring about multiple uncertainties, such as the fate of intermediaries that do not constitute PAs and how would they continue to function, especially since these Guidelines do not specifically repeal nor clarify to what extent it would override the Intermediary Directions.

Furthermore, as previously mentioned, the Guidelines are also unclear on the position and approach that existing PAs should take prior to obtaining an authorization, i.e. whether they should continue to comply with the Intermediary Directions or comply with the Guidelines by April 1, 2020.

Given that the Guidelines propose to bring about significant changes in the e-commerce industry and would change the way online payments are structured, it may be helpful if the RBI were to issue FAQs of its own, throwing light on various uncertainties and clearly explaining the position going forward for intermediaries and PAs.

— Aaron Kamath, Huzefa Tavawalla & Gowree Gokhale

126 Read our write-up on the data localization requirements applicable to payment system operators here.

Blockchain and Digital Assets

December 5, 2024

A. The Revolution Realized: Bitcoin's Triumph

Click the above logo to visit the published article

Sixteen years ago, it was nothing more than an audacious vision—a dream dismissed by the powerful and scoffed at by the wealthy. Back then, Bitcoin was derided as a scam, ridiculed as a Ponzi scheme, and disparaged as the modern-day tulip mania. The skeptics wrote it off, convinced it was doomed to fail.

But in the shadows of doubt, a resilient few dared to believe. They saw not worthless code, but the foundation of a revolution. These pioneers held firm, weathering the storm of criticism and standing unwavering against the tides of cynicism. They clung to their conviction that Bitcoin was more than a fleeting experiment—it was a new paradigm.

And now, that dream has silenced its doubters. Bitcoin, once dismissed as folly, has roared past the monumental milestone of $100,000 USD. Its value has surpassed that of a kilogram of gold, a testament to the strength of an idea whose time has come. This is no mere price point; it is a reckoning. A challenge to the traditional order. A declaration that decentralized power is here to stay.

Bitcoin's rise is not just about wealth—it is about trust reclaimed, freedom restored, and a system unshackled from the grip of intermediaries. It is a victory for those who dared to imagine a world where the individual, not the institution, holds the keys to their own financial destiny.

As the digital currency ascends, it carries with it a truth that can no longer be denied. Bitcoin is no longer just a dream; it is a force. It is proof that innovation, driven by purpose and belief, can rewrite the rules of the game.

It doesn't matter what the future holds—whether Bitcoin soars higher or retreats. The milestone of $100,000 USD is etched in history, a beacon for every skeptic turned believer and every doubter turned dreamer.

Bitcoin, you beauty, you have proven that revolutions are not born in the halls of power but in the minds of the daring. You have vindicated the faith of the few and redefined what is possible for the many. Wherever you go from here, your roar will echo through the ages.

— Suril N. Desai

November 14, 2024

B. The Bitcoin Effect

Click the above logo to visit the published article

Bitcoin. It's not just a perceived financial/investment asset; it's one of the most successful economic innovation in human history. This isn't just luck. It's the result of relentless work by miners, coders, hackers, and programmers around the world—people who took the idea of a decentralized currency and made it a reality. Bitcoin stands as the ultimate symbol of innovation. It rose quietly during the fallout from the 2008 financial crisis, as big banks failed, people lost homes, and the world became wary of traditional finance.

On Halloween night in 2008, Satoshi Nakamoto dropped the Bitcoin whitepaper into tech forums. It was open-source, global, and unstoppable. Suddenly, anyone, anywhere could help build and secure the Bitcoin network. This community of students, scientists, activists—and, yes, even the occasional shadowy figure—became the backbone of Bitcoin. And the code itself? Incredibly resilient. The Bitcoin blockchain has never stopped since its launch on January 3, 2009. In fact, the very first Bitcoin block contained a message from the Times (England), " Chancellor on brink of second bailout for banks." The timing couldn't have been more perfect.

At first, Bitcoin was misunderstood, mocked, and dismissed by governments, banks, and the media. Each time it was declared "dead," it returned stronger. This community—regular people, innovators, the curious—kept pushing forward, more resilient with each attempt to undermine it. Today, Bitcoin isn't just surviving; it's thriving. In fact, one Bitcoin can buy a kilogram of gold. Think about that—a digital asset created out of code holds value alongside gold, a centuries-old standard of wealth.

Bitcoin's capped supply of 21 million is a game-changer. In a world where fiat currencies are printed endlessly, Bitcoin is scarcity. It's a model of precision in a time of excess. While fiat supply increases exponentially, the amount of Bitcoin is locked, driving demand and giving it an intrinsic value.

Just imagine: the same asset that some people were handing out freely years ago—where 1,500 Bitcoins went for about a dollar—is now globally recognized, trusted more than some government-backed currencies. Bitcoin has even seen things like a Russian court fining Google an absurd USD 2.5 decillion— yes, that's a 1 followed by 37 zeros. In a world where governments print infinite currency, we're moving toward the scarcity Bitcoin represents.

With Bitcoin, we have a shot at a universal, decentralized pricing standard. We can quantify and measure anything, down to the atom. And here's the kicker: Bitcoin is a real force for good for those who believe in it. It's a silent revolution, showing the power of human intelligence and innovation. We've taken code and turned it into one of the most trusted assets on the planet. Bitcoin isn't just alive; it's leading the future.

— Suril N. Desai

March 13, 2023

C. Making Crypto Industry Compliant in India: A Welcome Move under the Anti-Money Laundering Laws

The Ministry of Finance **("MoF")** has recently extended the applicability of certain compliance obligations under the Prevention of Money Laundering Act, 2002 **("PMLA")** to various service providers in the virtual digital asset ecosystem (virtual asset service providers i.e. **"VASPs"**).

The PMLA stipulates measures to prevent money laundering and also provides for the confiscation of property involved in money laundering. In the recent past, authorities (such as the Directorate of Enforcement) have taken recourse under the PMLA against different VASPs in India including issuing orders freezing their assets.[1]

VASPs notified as Person Carrying on Designated Business or Profession

- The PMLA imposes due diligence and enhanced due diligence obligations[2] on specified "reporting entities" **("REs")**.[3] It also provides that any class of persons defined as a 'person carrying on designated business or profession' **("PCDBP")** is a RE for its purposes[4] and the central government is empowered to designate any person as a PCDBP. Accordingly, the MoF vide the notification dated March 7, 2023 **("Notification")** has specified a person who carries out the following activities for or on behalf of another person in the course of business as PCDBP:
  - Exchange of virtual digital assets ("VDAs") with fiat currencies or other VDAs;
  - Transfer of VDAs;
  - Provide safekeeping or administration of VDAs or instruments that enable control over VDAs; and
  - Participate and provide financial services related to an issuer's offer and sale of VDAs.
- Cryptocurrency exchanges, NFT platforms, cryptocurrency custody solutions and wallet providers, crypto lending and borrowing platforms, crypto launchpads, crypto payment gateways, crypto staking platforms and service providers facilitating initial coin/token offerings and executing SAFTs , are a few key businesses that will get covered under the definition of PCDBPs by virtue of the Notification.

1 Under PMLA, INR 936 crore related to crypto currency is attached/seized/freezed by ED as on 31.01.2023 - https://pib.gov.in/PressReleseDetailm.aspx?PRID=1896722.

2 Section 12 AA of the PMLA.

3 "Reporting entities" under section 2(1)(wa) of the PMLA is defined as "a banking company, financial institution, intermediary or a person carrying on a designated business or profession".

4 Other categories which fall under the PCDBP definition include (a) persons which carry out activities such as playing games of chance for cash or kind, (b) the Inspector-General of Registration appointed under the Registration Act, 1908, (c) real estate agents as notified by the government, (d) dealers in precious metals, precious stones and other high-value goods, and (e) persons engages in safekeeping and administration of cash and liquid securities on behalf of other persons.

Compliance Obligations on the Reporting Entities under PMLA and rules framed thereunder:

All REs including PCDBPs are subject to various compliance obligations under the PMLA and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 **("PMLA Rules")**:

- **Verification of Identity**[5]: Each RE is required to implement a know-your-client/customer (KYC) procedure to verify the identity of its 'clients'[6] and the 'beneficial owner'[7] using any of Aadhaar, Passport or other valid identity proof or mode of identification.

  The client due diligence needs to be carried out by a RE at two instances:

  - At the time of commencement of an account-based relationship[8]:
    - identify clients, verify their identity, obtain information on the purpose and intended nature of the business relationship; and
    - determine whether a client is acting on behalf of a beneficial owner, and identify the beneficial owner and take all steps to verify the identity of the beneficial owner.
  - In all other cases, verification of identity must be undertaken where a client carries out[9]:
    - a transaction equal to or exceeding the value of INR 50,000, whether conducted as a single transaction or several transactions that appear to be connected, or
    - any international money transfer operations.

  The RE is required to file an electronic copy of the KYC records with a Central KYC Records Registry (established under the PMLA) within 10 days of the commencement of the account-based relationship.[10]

- **Enhanced Due Diligence**[11]: In case of certain specified transactions[12] i.e., where the cash deposit or withdrawal, transaction in foreign exchange, high value import or remittance, exceeds the specified limit or where there is a high risk of money laundering or terrorist financing, the RE is required to carry out enhanced due diligence prior to the commencement of each such specified transaction, without which such transaction must not be permitted to be carried out. Such enhanced due diligence measures include:
  - undertaking identity verification of the clients before such transaction,
  - taking additional steps to examine the ownership and financial position of the client including obtaining information with respect to the source of funds, and
  - recording the purpose behind conducting the transaction and the intended nature of the relationship of the parties to the transaction.

5 Section 11A of the PMLA.

6 "Client" under section 2(1)(ha) of the PMLA is defined as "a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who engaged in the transaction or activity, is acting."

7 "Beneficial owner" under section 2(1)(fa) of the PMLA is defined as "an individual who ultimately owns or controls a client of a reporting entity or the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person."

8 Rule 9(1)(a) of the PMLA Rules.

9 Rule 9(1)(b) of the PMLA Rules.

10 Rule 9(1A) of the PMLA Rules.

11 Section 12AA of the PMLA.

12 As defined under explanation to section 12AA of the PMLA.

- **Maintenance of Records**[13]**:**
  - A RE is required to maintain a record of certain transactions for at least 5 years from the date of each such transaction [14], along with all necessary related information to permit the reconstruction of individual transactions.[15] These transactions include:
    - Cash transactions of a value exceeding INR 10 lakhs;
    - Series of cash transactions where individually each transaction may be less than INR 10 lakhs but the monthly aggregate value of such transactions exceeds INR 10 lakhs;
    - Suspicious transactions i.e. a transaction or an attempted transaction which to a person acting in good faith:
      - gives rise to a reasonable ground of suspicion that it may involve:
      - proceeds of a scheduled offence under the PMLA (irrespective of the transaction value); or
      - financing of activities related to terrorism; or
    - appears to be made:
      - in circumstances of unusual or unjustified complexity; or
      - have no economic rationale or bona fide purpose.
    - All cross border wire transfers of a value of more than INR 5 lakhs where either the origin or destination of the funds is in India.[16]

      The RE is also required to maintain a record of documents evidencing the identity of its clients and beneficial owners as well as account files and business correspondence relating to the clients for a period of five years after the business relationship between a client and the reporting entity has ended.[17]
    - Each RE needs to communicate to the authorized officer of the government (**"Authorised Officer"**) the name, designation and address of a designated director[18] of the board of the RE and the Principal Officer (an officer designated by the RE).[19]
  - The Principal Officer is required to furnish the information referred to in para B.3(a) to the Authorized Officer. Further, every RE is also required to develop an internal mechanism for detecting the above-mentioned transactions and furnishing information about such transactions.

13 Section 12 of the PMLA.

14 Section 12(3) of the PMLA.

15 Necessary related information includes (a) nature of the transaction, (b) amount of the transaction and the currency in which it was denominated, (c) date on which the transaction was attempted or executed, and (d) parties to the transaction.

16 Rule 3 of the PMLA Rules.

17 Section 12(4) of the PMLA.

18 The RE is required to appoint a Designated Director i.e. Managing Director or whole time director in case the RE is a company or a person designated by the RE to ensure overall compliance with the obligations with respect to maintenance and furnishing of records, and enhanced due diligence to be conducted by the RE.

19 Rule 7(1) of the PMLA Rules.

- The Principal Officer should furnish the requisite information to the Authorised Officer under the following timelines:
  - Suspicious Transactions: Within 7 days of being satisfied that the transaction is suspicious; Any other information should be furnished on a monthly basis, before the 15th day of the succeeding month.[20]
  - Maintain a record of documents evidencing the identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.[21]

Imposition of Fine and Bar of Proceedings

The Authorised Officer can inquire about the compliance status of the obligations on the RE on a suo moto basis or on an application made by any authority, officer or person.[22] Depending upon the nature and complexity of a case, the Authorised Officer may also order an audit of the records maintained by a RE.[23]

In the course of the inquiry, if the Authorised Officer finds that a RE or its designated director or any of its employees has failed to comply with the compliance obligations, then, he may—

- issue a written warning; or
- direct compliance with specific instructions; or
- direct submission of reports on the measures they are taking; or
- impose a monetary penalty on such RE or its Designated Director on the Board or any of its employees, which shall not be less than INR 10,000 but may extend to INR 1,00,000 for each failure.[24]

Except as provided above, immunity has been provided to the RE, its director and employees against any liability under a civil or criminal proceeding against them for furnishing above-mentioned information to the Authorised Officer.[25]

NDA analysis:

Although the Supreme Court of India in the IAMAI case affirmed the VASPs fundamental right to trade and do business, guaranteed under the Constitution of India, it has not been a smooth journey for the exchanges. These exchanges have been subject to investigations by various government authorities and their assets have been frozen in the course of their trade. The Notification is a positive step towards bringing more clarity on the compliance requirements. The VASPs will now be treated at par with financial institutions, banking companies, and intermediaries and will be subject to the rigours of the PMLA and PMLA Rules. This mechanism will ultimately benefit the entire ecosystem as the bad actors will be identified and eliminated, due to

20 Rule 8 of the PMLA Rules.
21 Section 12(1)(e) of the PMLA.
22 Section 13(1) of the PMLA.
23 Section 13(1A) of the PMLA.
24 Section 13(2) of the PMLA.
25 Section 14 of the PMLA.

the constant reporting of suspicious transactions. Further, the legitimacy of VASPs should also improve the customers' trust and help in attracting institutional capital.

The RBI in May 2021[26], had clarified to banks, payment system operators, and others **("Banking and Payment Sector")** that they may, continue to carry out customer due diligence processes with respect to the transactions involving virtual currencies, in line with governing standards and obligations of the regulated entities under the PMLA. Now with compliances to be carried out by VASPs under the PMLA read with PMLA Rules it would be interesting to see whether the taboo adopted against VASPs by the Banking and Payment Sector will reduce.

The VASPs operating in India will need to build in appropriate internal infrastructure in order to comply with the aforesaid requirements as conducting KYC and keeping a track of the transactions facilitated by the VASPs is no more a 'good to have' industry practice but a legal obligation. While VASPs may already have KYC policies in place, they will have to match them to the standards provided under the PMLA read with the PMLA Rules.

The extra-territorial application of the PMLA being ambiguous, the non-resident VASPs having an Indian user base should also take note of the Notification and build appropriate safeguards.

The Notification aligns with Nishith Desai Associates' previous recommendation submitted in 2017, a "Draft Code of Self-Regulation for Virtual Currency Businesses in India" **("Draft Code")** to an Inter-ministerial Committee which was set up to study virtual currencies.[27]

We recommended to the Inter-ministerial Committee that a self-regulatory code, such as the Draft Code, backed by a statutory mandate may be introduced imposing compliance obligations as per the KYC/AML norms prescribed under the PMLA.[28] Further in 2018, we had separately also suggested in our research paper "*Building a Successful Blockchain Ecosystem for India*",[29] that crypto business activity may be notified as a "designated business or profession" under the PMLA to mitigate money laundering risks. The Draft Code, inter alia, provided for a certification mechanism for a business that satisfied certain eligibility criteria and subjected them to compliances similar to those prescribed under PMLA such as maintaining records of the identity of customers, business activities and transactions, and reporting of materially non-compliant transactions.

The Draft Code, although voluntary and without statutory backing such as under the PMLA, was a first-of-its-kind in 2017. It was originally prepared for the Digital Asset and Blockchain Foundation of India (DABFI), which was later subsumed into the erstwhile Blockchain and Crypto Assets Council (BACC) of the Internet and Mobile Association of India (IAMAI).[30] Such measures helped businesses to demonstrate their diligence when called upon by law enforcement agencies and also helped in tracing/reconstructing suspicious transactions, identifying perpetrators and helping criminal proceedings. The Notification provides statutory recognition to these KYC/AML measures suggested before and ushers in uniform practices across the industry.

26 RBI/2021-22/45 DOR. AML.REC 18 /14.01.001/2021-22 dated May 31, 2021 - https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12103.

27 This committee comprised of members including from the Central Board of Direct Taxes (CBDT), the Ministry of Home Affairs, Ministry of Electronics and Information Technology (MeitY), Reserve Bank of India (RBI), and the National Institution for Transforming India (NITI Aayog).

28 See: https://news.bitcoin.com/indian-government-suggestions-cryptocurrency-regulation/.

29 See: https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Building-a-Successful-Blockchain-Ecosystem-for-India.pdf.

30 See: https://inc42.com/buzz/iamai-bacc-to-set-up-board-for-crypto-exchange-self-regulation/.

The regulators are further enabled under the PMLA read with applicable rules to issue enhanced or simplified measures to verify the client's identity. The RBI has already issued Know Your Customer (KYC) Direction, 2016[31] which applies to the Banking and Payment Sector.

It would be interesting to see if any regulator issues specific rules for VASPs or subject them to the existing regulations, especially in the case of the RBI, as it has been a strong advocate of banning crypto-related business, but would now have to adopt a balanced approach of regulation instead of prohibition.

The Indian government has been vocal about promoting blockchain, although heavily discouraging crypto at the same time. Further, in a few instances, the government has also suggested that it will await global consensus before passing any law regulating VDAs. However, lately, there have been a few changes introduced with respect to VDAs such as a new tax regime, reporting of VDAs under the Companies Act and now maintenance of records under the PMLA, which together have led to reducing uncertainty regarding the status of VDAs in India. These changes collectively may also be an encouraging opportunity for a new breed of service providers under the VDA ecosystem. However, ambiguity still exists on the overall regulatory direction of VDAs in India, and the introduction of a separate legislation/regulation for VDAs would be a step forward for the overall development of the industry.

— Vibhore Batwara, Purushotham Kittane, Alipak Banerjee & Vaibhav Parikh

31 See: https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566.

February 2024

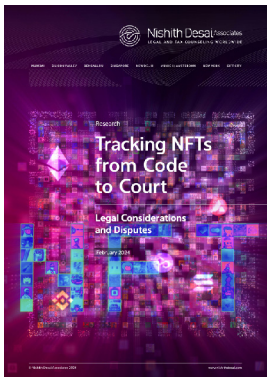
D. Tracking NFTs from Code to Court: Legal Considerations and Disputes

The research paper delves into the legal, technological, and regulatory dimensions of non-fungible tokens **("NFTs")**, offering a holistic perspective on their rising significance. The paper begins by unpacking the technological foundation of NFTs, highlighting the role of blockchain in creating unique, verifiable digital assets. It then transitions into a discussion on practical applications of NFTs, including in art, gaming, and digital ownership, amongst others.

A major focus of the paper lies in addressing the intricate legal challenges related to NFTs. It examines intellectual property issues, including copyright ownership and infringement risks. The authors also navigate the legal implications associated with the application of exchange control regulations, payment system laws and securities laws. Issues linked to anti-money laundering legislations and foreign direct investments are also discussed.

The paper critically evaluates the global regulatory landscape, identifying gaps and inconsistencies in how jurisdictions approach NFT-related disputes. It offers insights into how courts might adjudicate novel issues related to NFTs.

You may access the full research paper by scanning the QR code below:



February 2024

Tracking NFTs from Code to Court

Legal Considerations and Disputes

July 8, 2022

E. Taxation of Crypto-assets

The Income-tax Act, 1961 **("ITA")** did not contain any provisions for taxation of virtual digital assets **("VDA")** until the Finance Act, 2022 **("FA 2022")** (coming into effect from April 1, 2022). The Finance Act, 2022 has introduced the much-awaited taxation regime for VDAs in India. Specifically, FA 2022 introduced the following:

- Section 2(47A): An expansive definition for VDA;
- Section 115BBH: Taxation of income from the transfer of VDAs at the rate of 30%;
- Section 56(2)(vii) & (x): Gift tax on VDAs - definition of 'property' expanded to include VDAs;
- Section 194S: Withholding tax **("WHT")** provision on payment of consideration for the transfer of VDAs to residents.

Our in-depth analysis of the above-mentioned provisions at the time of their proposal through the Finance Bill of 2022, can be found here. Since then, certain changes were brought about in the provisions of the Finance Bill, through FA 2022, and more recently, the Central Board of Direct Taxes **("CBDT")**, and the Ministry of Finance **("MoF")** released a set of circulars and notifications to clarify the operability of the withholding provisions, the procedure for compliance, clarification on scope of VDAs etc.

In this hotline, we discuss and analyze the circulars/ notifications issued by CBDT.

Withholding on VDA Transactions through Exchange [Circular No 13 of 2022] ("Circular 1"):

Section 194S of the ITA obligates any 'person responsible for paying' to a resident any sum by way of consideration for transfer of a VDA to withhold tax at the rate of 1% at the time of payment or credit, to the account of the resident, whichever is earlier. Section 204 of the ITA defines the person responsible for paying to mean (i) in case of residents, the payer of the sum (or principal officer, in case of a company) and (ii) in case of non-residents, the person himself or any person authorized by the non-resident. In Uber India Systems (P.) Ltd.[32], the Income Tax Appellate Tribunal **("ITAT")** highlighted the distinction between payer and remitter and held that Uber India Systems Private Limited was not the payer, and consequently not the person responsible for paying.

Given the above, in case where an intermediary (like an exchange) is facilitating transfer of VDAs on its platform, it was not clear whether such intermediary could be held liable to withhold tax under section 194S.[33] To remove such ambiguities, Circular 1 clarifies who would be liable to withhold tax under section 194S in case where VDA transactions take place through an Exchange[34] or Broker[35] (as defined therein).

32 Uber India Systems (P.) Ltd. vs. Joint Commissioner of Income Tax, [2021] 125 taxmann.com 185 (Mumbai - Trib.).

33 https://www.theweek.in/news/biz-tech/2022/02/07/why-crypto-players-are-confused-about-new-tax-rules.html.

34 'Exchange' means any person that operates an application or platform for transferring of VDAs, which matches buy and sell trades and executes the same on its application or platform. The definition is wide enough to cover both models of exchanges typically seen in the marketplace.

35 "Broker" means any person that operates an application or platform for transferring of VDAs and holds brokerage account/accounts with an Exchange for execution of such trades.

The table below summarizes the clarification provided by Circular 1 with respect to the person responsible for withholding tax under section 194S.

S No	Consideration	Platform Model	Broker	Obligation to deduct tax
1.	Where consideration for the transfer is paid in fiat currencies	**Exchange Model** VDA (owned by another user/ Broker) transferred on the Exchange. The buyer and seller places orders on the Exchange platform. The Exchange matches and executes the order and earns in lieu of commission /service fee.	No broker involved	Tax to be deducted by the Exchange on the payment made to the seller (i.e. the owner of the VDA)
			Broker involved, where the broker holds title to the VDA (i.e. the broker is the seller)	Tax to be deducted by the Exchange on payment made to the Broker
			Broker involved, where the broker does not hold title to the VDA (i.e., the Broker is not the seller)	Obligation to deduct tax falls on both: (a) the Exchange, and (b) the Broker. However, Circular 1 provides that if there is a written agreement between the Exchange and the Broker that Broker shall be deducting tax, then Broker may deduct the tax under section 194S The Exchange will however need to furnish a quarterly statement for all such transactions in the quarter within the prescribed forms and due dates.
		OTC Model VDA (owned by Exchange) are transferred on the Exchange. The exchange is the counterparty to such transactions and maintains its own repository of VDAs and conducts back-to-back transactions with the users.	No Broker involved	Primary obligation to deduct taxes is on the buyer or their Broker (as the case may be). However, Circular 1 provides an alternative wherein the Exchange may enter into a written agreement with the buyer or their Brokers stating that the Exchange would be paying taxes. The Exchanges would be required to furnish quarterly statements for all such transactions. It will also be required to furnish its income tax return and include such transactions therein. Circular 2 provides that if these conditions are complied with, the buyer or his Broker would not be held as assessee in default under section 201 of the ITA for these transactions.
			Broker involved, however, the Broker does not hold title to the VDA (i.e. the broker is not the seller)	

Circular 1 also clarifies that in case of transactions where consideration for transfer of VDA is paid in exchange of another VDA, the Exchange would be required to withhold tax on both legs of the transaction. The buyer and seller would not be independently required to follow the procedure provided in provisio to section 194S(1).

It is important to note that Circular 1 has been issued under section 194S(6) read with section 194S(7) of the ITA. Therefore, Circular 1 is binding on the tax authorities and the person responsible for paying.

Our comments: The clarification provided by Circular 1 puts an end to confusion and extent of Exchange's liability to comply with section 194S. The compliance burden has been shifted from the users to the Exchange in most cases. Circular 1 also seems to have nailed practical issues faced by the industry. For example, it recognizes that there may be situations wherein tax deducted in kind may need to be converted into cash for depositing to the Government. In this regard, Circular 1 provides mechanism for tax deducted in kind into cash. The mechanism provided by Circular 1 is likely to increase the compliance burden on the Exchanges (with the Exchanges required to maintain trail of transactions, time stamping of order etc.). Further, the mechanism for accumulation of tax deducted in form of primary VDAs till end of the day and conversion into cash at midnight may provide opportunities to participants to engage in price play. This will need to be carefully monitored by Exchanges as well. In a welcome move, Circular 1 has also clarified that there will be no further withholding on conversion of tax withheld in kind into INR.

Withholding on Transactions not Covered Under Circular 1 [Circular No 14 of 2022] ("Circular 2"):

Circular 2 (except question 6) is applicable on all transactions not covered by Circular 1 i.e. transactions in relation to transfer of VDA not on or through an Exchange. Circular 2 inter-alia clarifies the liability to withhold tax in the following situations:

- *When the consideration is paid in fiat:* In peer to peer transaction (i.e. buyer to seller without going through an Exchange), the buyer (i.e. person paying the consideration) is required to deduct tax under section 194S of the ITA. The tax base for withholding is consideration for transfer of VDA as reduced by goods and service tax **("GST")**.
- *When the consideration is paid in kind:* In such a case, the person responsible for paying such consideration is required to ensure that tax required to be deducted has been paid in respect of such consideration, before releasing the consideration. Thus, the buyer will release the consideration in kind after seller provides proof of payment of such tax (e.g. challan details etc.).
- *When consideration is paid in exchange of another VDA:* In such a case, both the buyer and seller need to pay tax with respect to the individual transfer of VDAs. Once tax is pay, both the buyer and seller are required to show evidence to the other person so that the VDAs can be exchanged.

Without going into the merits of whether VDA is a good or not, Circular 2 also clarifies that once tax is deducted under section 194S, tax would not be required to be deducted under section 194 Q (withholding on purchase of goods).

Our comments: At the outset, it is important to note that unlike the guidelines issued Circular 1, Circular 2 has been issued under section 119 of the ITA. Therefore, while Circular 1 is binding on the tax authorities and the person responsible for paying, it may be possible to argue that Circular 2 is binding only on the tax authorities, and not on the taxpayers.[36] Having said this, it is not clear why Circular 2 was also not issued under section 194S(6).

36 See Navnit Lal C. Javeri vs. K.K. Sen, Appellate Assistant Commissioner of Income-tax, [1965] 56 ITR 198 (SC), Catholic Syrian Bank Ltd. vs. Commissioner of Income-tax [2012] 343 ITR 270 (SC) etc.

As discussed above, Circular 2 is applicable only on transactions not falling in the ambit of Circular 1. Therefore, in cases where VDA transactions are not happening through an Exchange, withholding under section 194S should be done in accordance with Circular 2. Further, while Circular 2 clarifies that tax base for withholding will be reduced by GST, applicability of GST on VDAs is not clear.

There have been news reports suggesting that Indian government is working on characterization of crypto-assets for the purpose of GST laws.[37]

Other Clarificatory Updates:

The CBDT also issued 2 other notifications, shedding further colour to the tax regime of VDA:

a. **Exclusions from the definition of VDA** *[CBDT Notification dated June 30, 2022]* **("Notification 3")**: Owing to the significantly wide definition of VDAs introduced through FA 2022, there was a lack of clarity as to whether airline reward points, credit card points, gift cards, etc. would also fall within the definition of VDAs. The Notification 3 excludes the following VDAs from the definition of VDAs:

   - Gift cards or vouchers, being a record that may be used to obtain goods or services or a discount on goods or services;
   - Mileage points, reward points, loyalty cards, being a record (i) given without direct monetary consideration under an award, reward, benefit, loyalty, incentive, rebate or promotional program (ii) that may be used or redeemed only to obtain goods or services or a discount on goods or services;
   - Subscriptions to websites or platforms or applications.

   Our comments: While the exclusions notified by the CBDT are welcome, it is important to note that the CBDT has worded the aforesaid notification in a narrow manner. The Notification 3 makes it clear that the items excluded earlier fell under the definition of VDAs. Having said this, it is important that emphasis is given to the exact language of the notification to determine whether the exclusion is applicable in case of a particular VDA or not. For example, in case where reward points are issued to users two conditions have to be satisfied for being excluded from the definition of VDAs – (i) the reward points should be given to the user without any direct monetary consideration under an award / reward program, and (ii) the reward point may be redeemed only to obtain goods or services or discount on goods or services. Therefore, in case where reward points can be used to obtain other cryptocurrencies or native / non-native tokens, it may not fall under the ambit of the exclusion depending on whether such cryptocurrencies or native / non-native tokens can be said to be 'goods' or 'services'. Pertinent to note that both Circular 1 and Circular 2 do not clarify whether VDAs will be characterized as goods for tax purposes or not. Same condition will have to be checked for gift cards or vouchers to qualify for the exclusion. Further, it is unclear why 'subscriptions to websites or platforms or applications' were required to be excluded from the definition of VDAs.

37 Available at: https://economictimes.indiatimes.com/news/economy/policy/govt-working-on-classification-of-cryptocurrency-under-gst-law/articleshow/90333798.cms (last accessed on June 08, 2022).

b. **Clarification with respect to the scope of Non-Fungible Tokens ("NFT")** *[CBDT Notification dated June 30, 2022]* **("Notification 4")**:

NFTs are specifically included within the scope of VDA as a separate category. Notification 4 specifies that a token which qualifies as a VDA is an NFT within the ITA.

However, an NFT whose transfer results in transfer of ownership of underlying tangible asset and the transfer of ownership of such underlying tangible asset is legally enforceable is excluded from the scope of NFT.

Our comments: The clarification provided under Notification 4 is welcome. NFTs generally represent a unique and existing physical or virtual goods, service or asset (e.g. artwork, music, real estate property etc.). It was not clear whether the tax department may view sale of an NFT as combination of two transactions – (1) sale of NFT itself, and (2) sale of the underlying property / asset represented by NFT. The clarification under Notification 4 should exclude cases where physical assets like land, painting etc. are tokenized and transferred through NFTs. Such NFT through which land or part of land is transferred and the ownership in the underlying land is also transferred will be excluded from the scope of VDAs. The sale of land will be taxable as per the usual provisions of the ITA and the VDA regime should not be applicable. This may give a boost to tokenization of physical assets. It is important to note that the Notification 4 covers only NFTs whose transfer results in transfer of ownership of underlying tangible (physical) assets. While practically ownership in underlying intangible assets (like music, video clip etc.) may not be transferred through NFTs, it will be important to closely examine the tax implications of such transactions as well.

Conclusion

The aforesaid clarifications, though last minute, have been welcomed by the industry participants. Several crypt-exchanges have implemented procedures to give effect and operationalize withholding from July 1, 2022. While the clarifications are technically applicable on foreign exchanges as well, foreign exchanges are likely to face more challenges in operationalizing withholding mechanism.

Having said this, the tax regime for VDAs is likely to evolve further in future. There are a number of open issues which continue to remain present. Currently, there are no guidelines on valuation of VDAs. This will be essential for determining tax base from income-tax and GST perspective. Valuation of VDAs may be particularly challenging given the volatility of the crypto-market. Lastly, the decision with respect to applicability of GST on VDAs may define the course of this industry in India.

— Arijit Ghosh & Ipsita Agarwalla

March 1, 2022

F. The RBI stand on Crypto lacks Balance

Click the above logo to visit the published article

A public authority has to be neutral and impartial. While some concern over cryptocurrencies is understandable, recently the Reserve Bank of India (RBI) compared crypto to a Ponzi scheme and the tulip bubble (or worse), and proposed an outright ban, a lack of balance.

Cryptocurrency is a platform technology. Like the Internet, they can be used for good and for bad. The Net facilitates child pornography and terrorism (and cryptocurrencies themselves), but no one seeks to ban it. Many of the criticisms of cryptocurrencies in the February 14 speech of the RBI deputy governor apply equally to the internet. Like crypto, the net can also be linked to an anti-establishment ideology. Remember John Perry Barlow's 1996 Declaration of the Freedom of Cyberspace, which asked governments to leave the trap alone? Cryptocurrencies are criticized for being global, decentralized and bypassing middlemen. But why should it be bad? Email is global, it obfuscates the post office, and it's useful. We are reminded of a 1995 Newsweek article that said this about the Net: "We've been promised instant catalog shopping – just point-and-click for great deals. ...so how about my local mall Does more business in an afternoon than the entire Internet handles in a month?"

One does not expect RBI to praise the cryptocurrency, but one expects it to take a balanced approach, so that it does not gloss over the pros and only highlight the cons.

The speech's argument that cryptocurrencies cannot satisfy any requirements in the financial sector can be dismissed. According to World Bank data, India was the largest receiver of inward migrant remittances worth $87 billion in 2021. But the average cost of sending remittances to India in 2020 was 5.4%. it over. translates into 30,000 crores in cost, almost three times our annual midday meal budget. Given the permissible regulations, this money can be saved, as many cryptocurrencies allow cross-border transfers within seconds at near-zero costs. Cryptos have proved useful in many other contexts as well, including the World Food Program and power schemes by UNICEF and helping to raise thousands of crores for COVID relief in India. In fact, despite speech claiming that a crypto ban will not harm blockchain technology, it fails to note that many 'blockchain' innovations are powered by native cryptocurrencies, such as the Maharashtra State Board of Justice based on Ethereum. Certificate verification program of skill development, and non-fungible token (NFT) offerings by Indian creators and media houses. While the largest global institutions and academics, including Turing Award winners, and some of the best Indian minds acknowledge the technological success of cryptocurrencies, the RBI remains in disbelief.

Some relevant facts were also missed in the speech. Citing a source that estimated the value of crimes using cryptocurrencies globally at $14 billion in 2021, it did not note that the same source found that illegal activity accounted for just 0.15% of total crypto transaction volume. The speech also said that illegal transactions have been "largely filtered out of the formal financial system", but did not cite the RBI's own annual report, which found that the total amount of fraud in the Indian banking system in 2020-21 was over. 1.38 trillion (which is over $14 billion). Still, no one would call it a "ponzi scheme".

Even though RBI wants to express a strong dislike for cryptocurrency, a ban call disregards our constitutional plan. It is a basic constitutional principle that the state does not decide private matters for its citizens. In a famous case on the right to privacy, the Supreme Court declared, "The best decisions on how life should be lived are left to the individual." Citizens have the right to participate in a new technology wave and be a part of what is. Known as the Fourth Industrial Revolution. Millions of Indians are doing this. The RBI had already made a caustic claim in the Supreme Court defending its 2018 circular on virtual currencies, which the court found lacking empirical basis, disproportionate and therefore unconstitutional. A long line of cases has assumed there is a high bar for the state to ban something. Mere dislike is insufficient. The speech had no underlying economic data, including any projections, to show how cryptocurrency is actually "ruining" the economy. which has been mentioned that regulation cannot solve. The speech asked how the case of mis-selling would be redressed if the cryptocurrency was not banned. Some research suggests that crypto-currency fraud cases have already been prosecuted in India. In fact, law enforcement agencies use a combination of publicly available blockchain logs and information gathered from exchanges and banks to trace criminals. The ban would deprive law enforcement agencies of this information.

The outright ban on cryptocurrencies is likely to be excessive and unconstitutional. Even in the winter session of Parliament, the finance minister said the previous draft proposing the ban was being reworked. The chairman of the committee which made this proposal also now advocates regulation instead of prohibition. Therefore, it is expected that the RBI will reconsider its extreme stance. Meanwhile, India may need to set up a crypto regulatory and development authority—say, a multi-stakeholder regulatory authority with expertise in computer science, regulation and economics—that can help us move the conversation forward.

These are personal views of the author.

— Nishith M. Desai and Jaideep Reddy

February 4, 2022

G. NFTs through IPR lens

Non-fungible tokens a.k.a. NFTs have taken the media industry by storm. From Big B- Amitabh Bachchan to the one and only Bhai- Salman Khan to singers like Sonu Nigam to cricketer-cum-celebrities Yuvraj Singh, and production houses like Viacom, there are now enough and many examples of the media industry foraying into this space. There is no dearth of variety either. Drawings, cartoons, caricatures, and posters (artistic works), songs and tunes (musical works), scripts and dialogues (literary works) and films themselves (cinematographic work) are being sold as NFTs. Options are limitless. Our Indian film industry is fully aware of this. Hence the need to understand the issues related to rights in NFTs.

Creating NFTS From Existing Works

The (Indian) Copyright Act, 1957, like most copyright legislations around the world, defines copyright widely. All modes and mediums of exploitation of a work are considered as "rights" . Due to the wide definition, copyright is considered a bundle of rights and each right within the bundle is capable of separate ownership or license. Creating of NFTs in relation to copyrighted works is also one of the rights from this bundle.

Thus far, media contracts were not negotiated to specifically call out the right to create and sell NFTs. This is changing. Now stakeholders are starting to negotiate NFTs as a specific right. It would be interesting to see how existing contracts get interpreted i.e. who will be considered to have that right. E.g. if a producer has granted digital right to a streaming platform, would such streaming platform have a right to create NFT as well because NFT could be construed as falling within definition of digital rights. This will depend upon the manner in which the definitions and clauses are drafted.

It is therefore important to review chain of title documents carefully to determine what rights have been given to which party, to avoid legal actions. Quentin Tarantino's legal dispute with Miramax over Pulp Fiction is an interesting precedence in this space.[38]

When a NFT is made of a video clip where a performer or sports personality is included, the agreement with such individuals should also be examined. E.g. usually, performers grant a right to use their attributes, caricature, voice, etc. in relation to the working which their performance will be used such as the film, web series, interview, etc. Hence, separate permission may not be required from the performer. However, if the performer has reserved some rights (example, gamification or merchandising rights) then the use of NFT has to be seen to evaluate if a permission is needed or not. The performer may also ask for share of consideration received from the sale of the NFT, including subsequent sales of that NFTs. If the NFT is used to endorse a product or brand that may lead to separate commercial negotiations.

If you are not the owner of the original work, but want to create a NFT based on a work that you have identified (say a poster of a film), then you need to approach the appropriate right holder for permission to create the NFT. Else, you could be infringing someone's copyright and heading for a dispute.

38 See Miramax Sues Quentin Tarantino Over Pulp Fiction NFTs | Time.

Buyers Rights

Buyer has limited rights in the NFT. Comparing this to a real world scenario, a buyer of a prized painting typically has the right to say he/she own it (bragging rights), display or exhibit it, and to even sell it onwards. The buyer does not get the right to make copies of the painting, or monetize it in other mediums-such as printing it on tshirts etc. The same logic applies to NFTs as well since it is nothing more than a digital copy of a work.

Newer models are developing quickly in this space and sometimes the buyer may also get the right to earn from the investment made in the NFTs. An example is of the Blockchain-based music investment platform Royal will let fans invest in hip-hop legend Nas music on the platform.[39] Investees in NFTs issued for the song will receive is a share from royalties every time the music is streamed. Thus, they are stakeholders in money earned from exploitation of the song, though not the owners of the IP in the song. This is similar to investing in mutual funds. The fund invests your money in various securities and pay earnings to you. It does not make you the owner of the security in which the money is invested.

Trademarks and NFTs

NFTs are a product offering. They can have a name – which could be a trademark. They can also incorporate a trademark -for instance a film, image, or song may include a brand name in it. If such use of trademark or brand is unauthorized, then it could result in exposure to a trademark infringement or passing off suit. There is already precedence in the west on unauthorized trademark usage in NFTs.[40] Brand building is a time and capital intensive exercise. Many organizations take protection of their brands very seriously. Hence, it is important to clear use of trademark before incorporating or using it for a NFT.

Legal Action

A claim will lie against the creator of the infringing NFT at the first instance, especially if the creator retains the intellectual property **("IP")** rights in the NFT. At times, ell the NFT platform may be impleaded as well (for facilitation such infringement) in a legal action. Since most NFT platforms are marketplaces which are only providing a platform for sale and purchase of NFTs, they are likely to qualify as intermediaries under the Information Technology Act, 2000. As such, they will be able to take safe harbour and defend a liability as long as they take down the infringing content upon receipt of actual knowledge by way of a government authority or court's order.

A Word of Advice

NFTs are a new medium of exploitation of work. Hence, a through diligence of chain of title documents is important to ascertain that the NFT seller has the rights to create, and sell the NFT.

39 See: https://www.lexology.com/library/detail.aspx?g=92d81306-ca86-47ca-b570-34ad16483039.

40 https://indianexpress.com/article/explained/hermes-lawsuit-metabirkins-mason-rothschild-nft-7736973/.

IP centric representation, and indemnities should also be built in the smart contracts meant for sale of NFTs from a buyer protection perspective. Blockchain will make the examination of chain of title easier for subsequent sales but won't rescue at the listing stage. Hence the need for diligence, else there could be several IP related claims which would in turn have a negative impact on NFTs overall.

— Aparna Gaur, Aarushi Jain & Gowree Gokhale

November 30, 2021

H. Don't ban cryptocurrencies, instead set up a regulatory body

Firstpost.

Click the above logo to visit the published article

Whether you are for or against bitcoins and cryptocurrencies, you cannot deny their importance as an evolution in money and banking. In a short span of 13 years, cryptocurrencies have gained mass acceptance and popularity, paving the path for a more inclusive economy. According to the *CNBC Millionaire Survey 2021*, nearly half of the millennial millionaires have at least 25 percent of their wealth in cryptocurrencies. There are approximately 150-200 million crypto users worldwide and about 15-20 million in India, according to Nischal Shetty, CEO of WazirX. Not all are drug peddlers or terrorists. Many of them are highly sophisticated and reputed investors. This means a large number of people have seen the benefits of investing in crypto.

Before considering a ban, it must be inquired as to why people are valuing cryptocurrencies so highly and what benefits they perceive. It should not happen that years later, we find that India has missed being part of a major financial revolution. The government's decision has to be evidence-based. Legislators must study the approaches taken by various countries prior to coming out with a regulation.

There is absolutely no denying that crypto has been used for illegal purposes, but so has cash or 'fiat'. All technologies are a double-edged sword. The same knife that is used to cut vegetables can be a murder weapon. To pass the entire burden of terror financing onto crypto is simply unfair. In 2012, HSBC admitted to moving large sums of dirty money for Mexican drug cartels and paid a hefty fine for doing so. At the time, none of our politicians debated about banning the banking system, so why do they give this step-sisterly treatment to crypto?

It is clearly evident that cryptocurrencies are going to disrupt the banking and monetary system, just like email disrupted the postal and telegraph service. Presently, the gatekeepers are trying to stop change instead of adapting to it. Rather than banning crypto, it is important for governments to nurture it and let it evolve. India is strategically poised to capitalise on this technology. Our great country has one of the largest talent pools of innovators, especially in the IT sector. India is also home to some of the best programmers in the world and leveraging their skills could make us a powerhouse in blockchain technologies. A liberal framework would put India's economy into hyperdrive and speed up the goal of a $5 trillion economy.Conversely, if cryptocurrencies are banned, India will witness a mass exodus of highly talented innovators, programmers and computer scientists. The first casualty would be the 'crypto miners' and software developers. Public blockchain cannot survive without an incentive mechanism, which cryptocurrencies provide. Foreign blockchain companies that have subsidiaries in India would have to move away from India.

New Indian blockchain enterprises will have to be incorporated outside, hence Indian IP would be lost in addition to tax revenues. We will lose the ability to raise global capital by way of legitimate token issuance.

So, where is the value of crypto for India? Most immediately, it eliminates intermediary costs. Today's banking system is designed for the rich. If you are sending millions of dollars across borders the banks charge a much lower transaction fee, while the transfer costs for small amounts could be as high as 7-10 percent. This has a direct effect on the foreign remittances market, which brings close to $75 billion from the Indian workers abroad. Crypto can save India a sum of $7.5-10 billion in transaction fees. This amount can possibly be used to fund the entire mid-day meal programme for the nation.

The potential of crypto is enormous and banning it would be throwing the baby out with the bathwater. We must prevent its nefarious uses through regulation. In its judgement of March 2020, the Supreme Court has already said that banning cryptocurrencies is extreme and unconstitutional, and regulating the space would be more appropriate. We can't ban technology, but we can certainly regulate the behaviour of the actors. Just imagine, what would have happened to India if the Internet and websites were banned?

Crypto is driving huge growth in the Indian technology ecosystem. Two of India's 31 unicorns are crypto companies. A recent report by NASSCOM found 32 potential benefits of the crypto technology for the citizens, industry and the Indian economy. The report states that the industry currently provides employment for 50,000 individuals in India and that there are $6.6 billion worth of investments in crypto assets by retail investors in India.

The report projects that by 2030, the industry can create eight lakh plus jobs in India and can potentially create an economic value addition of $184 billion in the form of investments and cost savings. This would also create corresponding tax revenue for the government.

Non-Fungible Tokens have helped small and medium creators access a worldwide market for their work. NFTs reside on public blockchains like Ethereum. To create and transfer NFTs, participants need to pay network fees in crypto. Without crypto, therefore, NFTs cannot be successful in India.

Cryptocurrencies have also proven to be socially beneficial. India Crypto Covid Relief Fund (which gathered donations in crypto-assets from all over the world) has donated over $36 million/Rs 270 crore. towards Covid relief in India, with another $429 million pending donation. UNICEF launched a 'Crypto Fund' allowing it to receive and disburse cryptocurrencies to fund projects in emerging markets. The World Food Programme is using cryptocurrency networks to expand refugees' choices in how they access and spend their cash assistance.

It is understood that the government is planning to come out with a Central Bank Issued Digital Currency (CBDC). Indeed, they should experiment with it but banning other decentralised cryptos would be inappropriate. Let there be fair competition. Both approaches are based on 'trust', there is no tangible asset to back them. People will decide and adopt the ones in which they have greater trust and faith.

Indeed, both should have an enabling and promotional regulator along with the lines of Insurance Regulation and Development Authority (IRDA). Is it the right time for a Cryptocurrency Regulation and Development Authority (CRDA)?

— Suril Desai

September 23, 2021

I. Blockchaining Education- Legal nuances to know

The last few years have seen an unprecedented increase in the use of technology across sectors. The education industry in particular has adapted well to this change. It has integrated technology almost seamlessly into its existing frameworks, both for the delivery of course content and ancillary objectives like administrative tasks and solutions for paying fees. One such new, upcoming and revolutionary technology is blockchain, which offers potentially great solutions to the education sector, for storing certificates, verification of credentials, rewarding students for task completion and intellectual property management, et al.

What is Blockchain?

Fundamentally, a blockchain is a decentralised network facilitating transactions between multiple participants usually across different locations. It stores a record of all transactions which occur on it in separate "blocks". It is 'decentralised' because these records are distributed across devices of each participant in the network, and no single entity controls the network, unlike traditional databases. In the case of public blockchains, this data can be accessed by anyone with an internet connection, while private blockchains generally require participants to provide a security key before they can access the blockchain database.

Blockchain offers a unique way for securing data through a decentralized system, and this storage is immutable in nature, meaning that data once stored on the blockchain cannot be removed, tampered with or altered by third parties. For instance, if a document is stored on a blockchain network in block "A", a change made to this document would create an entirely different block "B", making it possible to identify and track all changes made to the document in a secure manner.

Although blockchain came into vogue primarily as part of cryptocurrencies like Bitcoin, the distributed manner of storing information used by blockchain systems has several other uses which go much beyond payments and trading.

How can it be used in the Education Sector?

The need to expand use blockchain technology in the education sector has been acknowledged by the government in the National Education Policy, 2020 **("NEP")**. The NEP lists blockchain as one of the emerging technologies which will likely gain prominence in the education sector in the near future.[41]

41 National Education Policy, 2020 at page 56,: https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English_0.pdf, (last accessed on September 21, 2021).

i. *Student Identity Verification*

The permanent and highly secure nature of data stored on the blockchain can be leveraged by schools, colleges and universities to assign an identity to their students. A digital identity which is created for a student on the blockchain could have numerous benefits as well. It would enable schools and universities to easily create a record of a student, and to update their records in a secure manner.

This digital identity can also be used by students as an all-access pass to use all virtual resources being offered by an institution. The key advantage of integrating the blockchain to verify student identities is that: (a) it is highly secure compared to digital solutions currently in the market; and (b) advancements of students can be easily tracked on the blockchain by studying the newer blocks added on the chain.[42]

ii. *Authentication of university degree and certificates*

As an example, the Massachusetts Institute of Technology (MIT) has been using blockchain technology to issue certificates to its students since 2015.[43]

In India as well, the use of blockchain in issuing authenticated and secure university certificates is being explored by an initiative called the SuperCert, a collaboration between the NITI Aayog and the Indian School of Business.[44] This platform has been proposed to issue course certificates through a permissioned blockchain architecture. Through SuperCert, each student is assigned a unique identity, which may be used by employers to verify the authenticity of their certificates. This system creates a fingerprint, or a hashed version of the certificates that are uploaded on the blockchain. At the time of verification, the SuperCert system compares this hashed fingerprint of the original certificates with the certificates provided to employers by students. Employers are informed in case any discrepancy is detected in the document provided by students. Such a system ensures that the privacy of students is protected (since employers do not access the original certificates which remain with the university), without compromising the authenticity of certificates.

In a recent development, the Maharashtra Government has announced that it intends to use an Ethereum-based blockchain network to verify student diplomas issued by the Maharashtra State Board of Skill Development **("MSBSD").**[45] This marks a first in the country, and it is expected that almost one million certificates will be issued in connection with this project. However, unlike the proposed SuperCert solution which relies on a private blockchain, the MSBSD's use of the Ethereum network to implement verification solutions will be on a public, permission-less blockchain, and interestingly, requires the use of 'Ether' a cryptocurrency / crypto-asset, to function.

Such usage of blockchain to verify certificates streamlines the process of issuing certificates by reducing the procedural formalities around it. It also significantly decreases the expenses incurred by educational institutions in issuing certificates and degrees, while ensuring the security of the document at the same time.[46]

42 Andrew Tobin, Jamie Smith, Self-Sovereign Identity for Higher Education,: https://www.evernym.com/blog/self-sovereign-identityhigher-education/, (last accessed on September 21, 2021).

43 Elizabeth Durant, Alison Trachy, Digital Diploma debuts at MIT,: https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-usingbitcoin-blockchain-technology-1017, (last accessed on September 21, 2021).

44 NITI Aayog Draft Discussion Paper, Blockchain: The India Strategy, January 2020.

45 Ledger Insights, Indian state government launches blockchain educational certificates, ledgerinsights.com/indian-state governmentlaunches-blockchain-educational-certificates/,(last accessed on September 21, 2021).

46 Rachel Wolfson, US Education Department Promotes Putting Student Records On Blockchain: https://cointelegraph.com/news/useducation-department-promotes-putting-student-records-on-blockchain, (last accessed on September 21 , 2021).

iii. *Tokens as Rewards for Task Completion*

Another application that blockchain technology has in the education sector is through initiatives like "BitDegree"[47]. BitDegree is an example of a Massive Open Online Course **("MOOC")**, and employs a "learn to earn" model. It uses the public Ethereum blockchain to build tokens which are used to incentivise its users who learn certain skills. Such tokens have limited uses, such as taking paid courses at educational institutes.

iv. *Intellectual Property Management*

Management of intellectual property in the context of academic research is a key application of blockchain. One such example is "Ledger", a peer-reviewed scholarly journal published online by the University Library System, University of Pittsburgh[48]. It allows users to digitally sign their documents using their bitcoin private keys, and timestamp published manuscripts in the blockchain. Such systems are helpful in automatically tracking the originators of documents and identifying authors. Since data stored on the blockchain is permanent and tamperproof, it is ensured that the integrity of academic research is preserved in a secure manner.

v. *Payments*

Blockchain technology may also be used by educational institutions to accept cryptocurrency payments from students as a safe and secure alternative to the traditional methods of payment, depending on the regulatory landscape for such methods in the relevant jurisdiction. Several universities across the world have begun to accept cryptocurrencies as a valid mode for the payment of tuition fees.[49]

Legal and Regulatory Challenges

i. *Privacy and Data Protection*

Widescale adoption of blockchain technology will certainly revolutionise the existing framework of the education sector. However, considering that this will involve the storage of highly sensitive personal data of students on a decentralised network, educational institutions should ensure that they take all possible measures to protect the information of their students on the blockchain.

The current regulatory landscape on data protection in India is governed by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 **("SPDI Rules")**. The SPDI Rules define sensitive personal data to include information such as financial information, medical records, biometric information, etc. Under the SPDI Rules, body corporates which collect, receive, possess, store, deal or handle sensitive personal data of others, in an electronic form, must follow the requirements under these rules, which inter alia include obtaining consent for collecting such data from the providers of information and refraining from retaining the sensitive personal data for longer than required for the purpose of such collection.

The SPDI Rules will likely be applicable where data about student identities and degree certificates is made available on the blockchain. This is because such data is could include , biometric information and financial data, which is treated by the SPDI Rules as "sensitive personal data."

47 https://www.bitdegree.org/, (last accessed on September 21, 2021).

48 https://ledgerjournal.org/ojs/ledger/about, (last accessed on September 21, 2021).

49 Universities Accept Bitcoin Payments to Ease the Burden on International Students,: https://www.analyticsinsight.net/top-universities-and-schools-accepting-bitcoin-payments/, (last accessed on September 22, 2021).

To comply with these requirements, any educational institution seeking to use blockchain networks for document verification will have to inform students (a) that this data is being collected to facilitate future verification, and (b) that data once stored on the blockchain cannot be removed.

The SPDI Rules also mandate that certain reasonable security practices are to be established when sensitive personal data is collected.

The SPDI Rules further provide certain examples of standards which would be considered sufficiently reasonable.[50] Where universities are relying heavily on the blockchain to store student data, there is no clarity if such standards under the SPDI Rules can be considered to be satisfied. This is because these requirements under the SPDI Rules have been targeted at systems which store personal data in a single location. However, data on blockchains are stored in a decentralised and distributed manner, meaning that it may be practically impossible to implement these specific security standards in the systems of all participants on the blockchain network.

ii. *Spill-over effects of a potential cryptocurrency ban*

Recently, it was reported that, pursuant to an Inter-Ministerial Committee recommendation of 2019, the Indiangovernment is considering a ban on dealing with all private cryptocurrencies.[51] However, in this context, the latest statement of the Finance Minister has been that "a futuristic thing can't be shut out".[52] The matter is reportedly pending consideration of the Union Cabinet.[53] A ban on cryptocurrencies may affect digital assets, including those generated by MOOCs such as BitDegree to reward students completing tasks successfully, as well as a pioneering program like that of the MSBSD, as discussed above.

Experts have opined that it may be difficult to separate blockchains from cryptocurrency.[54] This is becauseblockchains usually reward participants on the chain for expending energy to authenticate transactions by giving them crypto assets. Without such crypto assets, participants on the chain may not be incentivised to validate entries in the distributed blockchain ledger. Hence, a potential ban on cryptocurrencies may severely limit the use of blockchain technology for many of the purposes outlined above.[55]

One such example of a system which may be negatively impacted by a ban on cryptocurrency is that of the recent solution for certificate verification introduced by the Maharashtra State Government discussed above. Since this solution uses Ethereum, a public blockchain which relies on cryptocurrency to function, a crypto ban is likely to impede this initiative and restrict access to the certificates uploaded on the blockchain.

50 IS/ISO/IEC 27001 standards on Information Technology - Security Techniques - Information Security Management System –Requirements.

51 The Indian Express, RBI plans and an upcoming Bill: Where are digital currencies headed?: https://indianexpress.com/article/explained/cryptocurrency-bitcoin-rbi-7285249/, (last accessed on September 21, 2021).

52 Hindustan Times, On Cryptocurrency, Sitharaman Says 'We Have To Be Cautious But Think It Through',: https://www.hindustantimes.com/business/on-cryptocurrency-sitharaman-says-we-have-to-be-cautious-but-think-it-through-101632189095218.html, (last accessed on September 22 , 2021).

53 Economic Times, Waiting for Cabinet approval, says FM Nirmala Sitharaman on bill on cryptocurrency,: https://economictimes.indiatimes.com/news/economy/policy/waiting-for-cabinet-approval-says-nirmala-sitharaman-on-bill-oncryptocurrency/articleshow/85372886.cms?from=mdr.

54 Russia's Crypto Ban Would Stifle Blockchains,: https://news.bitcoin.com/buterin-ban-russia-stifle-blockchains/, (last accessed on September 21, 2021).

55 Note: Initiatives like SuperCert may not face this issue, since they rely on a private/permissioned blockchain, meaning that all participants on this chain can be identified by the central authority. The spillover effect may hence be a significant issue only where universities are taking resort to public blockchain structures. See: https://www.steptoe.com/images/content/1/8/v2/189187/Cybersecurity-Tech-Basics-Blockchain-Technology-Cyber-Risks-and.pdf,(last accessed on September 21, 2021).

iii. *Cybersecurity*

Though the data storage and verification on the blockchain has been touted to be one of the most secure means ever devised, cybersecurity vulnerabilities are not entirely eliminated. For instance, there have been several recent situations where hackers gained unauthorised access to information on the chain, and exploited the information contained therein.[56] Though this is technically more difficult to achieve than by hacking traditional centralized systems, blockchain networks do have some vulnerabilities which may be exploited.
For example, where blockchain networks rely on a majority consensus mechanism (meaning that a transaction on the blockchain is authenticated if more than 50% of the computing power of the network has authorised it), it would be possible for hackers to take over this system by gaining control of more than half of all the computing power on the network. This could have disastrous results where universities and other educational institutions rely on the blockchain to store and authenticate student information especially where the personal data of students is concerned.

To manage the risks presented by such eventualities, universities should implement strong cybersecurity frameworks including negotiating contractual protections with other participants and undertaking continuous monitoring of the network for security incidents.[57] In addition, such institutions should also ensure that they comply with requirements under the Information Technology Act, 2000 of India and similar laws which require body corporates to report unauthorised uses of computer resources to the relevant authorities within a reasonable timeframe.[58]

Our Take

The blockchain technology offers significant advantages to the education sector across the globe and couldsignificantly decentralise and democratise access to education. In India, particularly, the opportunities offered by blockchain technology in the sector are only beginning to be explored by the government and private players alike. This also offers opportunities for new and allied business models in the education space.Further, the government has presented a positive outlook towards the use of blockchain technology for improving education in the country under the NEP. We foresee more acceptability and adoption of blockchain in education in the new future.

— Athira Sankar, Jaideep Reddy & Aarushi Jain

56 MIT Technology Review, Once Hailed As Unhackable, Blockchains Are Now Getting Hacked,: https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/, (last accessed on September 21, 2021)

57 https://www.steptoe.com/images/content/1/8/v2/189187/Cybersecurity-Tech-Basics-Blockchain-Technology-Cyber-Risks-and.pdf, (last accessed on September 21, 2021)

58 See Reporting cybersecurity breaches in India – Is it time to overhaul the law?,by Aparna Gaur, Aarushi Jain, Gowree Gokhale and Dr. Mihir A. Parikh, available at: https://www.natlawreview.com/article/reporting-cybersecurity-breaches-india-it-time-to-overhaul-law, (last accessed on September 21, 2021).

April 26, 2021

J. Taxing Non-Fungible Tokens

Non-fungible tokens **("NFTs")** are digital tokens that operate on a public blockchain and can be used to represent ownership of a unique item, whether digital or physical. Each NFT is unique and unlike other fungible assets or currencies, they cannot be exchanged with one another. NFT products can be representative of a variety of elements and can tokenise things like art, collectibles and fashion items to collectible sports cards, virtual real estate and characters. Globally recognized brands like Nike, Louis Vuitton, as well as the NBA have begun generating NFT-based consumer goods and services.[59] IBM has recently announced that it will turn corporate patents into NFT so that the patents can be easily sold, traded or otherwise monetized.[60] NFTs have the potential to create a paradigm shift by creating an 'Internet of Assets'.

NFTs can either be created by developers or by users through third-party marketplaces. NFT marketplaces such as OpenSea, Rarible or Nifty Gateway facilitate the online sale of items through the use of NFTs to represent title or ownership. A typical NFT marketplace transaction begins with the seller "minting" an NFT to represent ownership of the unique item that they wish to sell. The seller then lists the item on the marketplace. Both stages require payment of a "gas fee", which users are responsible for paying towards the computing energy required to validate transactions on the blockchain. The gas fees fluctuate depending on the time of day and is sent directly to miners who run the blockchain network.

Once the item is listed on the marketplace, a buyer may either purchase it directly or place a bid in an auction. The buyer pays the consideration amount, the gas fees, and the commission charged by the marketplace. The entire transaction usually takes place through the operation of a smart contract where payments are automated and made directly between parties instead of through the intermediary NFT marketplace. As a result, the marketplace does not have access to any amount paid by the buyer except for its sales commission. More than $2 billion was spent on NFTs in the first quarter of 2021 – representing an increase of about 2100% from last quarter of 2020.[61] Given this recent surge, we have summarized the potential tax implications of such transactions in this hotline.While the tax treatment of NFTs should generally depend on the nature of the underlying asset, there may be other issues in case of cross-border NFT transactions.

Equalization Levy

The Finance Act, 2020 expanded the scope of the equalization levy **("EL")** to be applicable on e-commerce operators at rate of 2 percent on the consideration received or receivable by such e-commerce operators from 'e-commerce supply or services' made or provided or facilitated by it to specified persons. Accordingly, the NFT marketplaces may be subject to EL at rate of 2% if it receives consideration from 'e-commerce supply or services' made to a person resident in India, a person using an Indian internet protocol **("IP")** address, or a non-resident in certain specified circumstances.

59 Kay, Grace. (2021, March 3). What you need to know about NFTs, the collectible digital tokens that are selling for millions online. Business Insider.: https://www.businessinsider.in/tech/news/what-you-need-to-know-about-nfts-the-collectible-digital-tokens-thatare- selling-for-up-to-millions-online/articleshow/81199814.cms.

60 Chipolina, Scott. (2021, April 21). IBM Is Turning Patents Into NFTs. Decrypt.: https://decryptco.cdn.ampproject.org/c/s/decrypt.co/68501/ibm-is-turning-patents-into-nfts?amp=1.

61 Burch, Sean. (2021, April 3). NFT Market Surges 2,100% to $2 Billion in Q1 Sales. The Wrap.: https://www.thewrap.com/nft-marketsurges-2100-to-2-billion-in-q1sales/#:~:text=More%20than%20%242%20billion%20was,a%20new%20report%20NonFungible.com.

The term 'e-commerce supply or services' has been defined very broadly such that it is not necessary that the entire transaction takes place online. The e-commerce operator would be subject to EL even if one of the aspects of the transaction, such as acceptance of offer of sale or placing of purchase order or payment of consideration, etc. takes place online. In relation to the tax base, the Finance Act, 2021 has clarified that the EL would apply on the entire consideration received from the buyer, and not just the commission amount retained by the e-commerce operator.

Applying this provision to the purchase of NFTs would lead to certain complications.

Firstly, the definition of ecommerce operator under the EL provision is very wide and may extend to any electronic service which may facilitate a buyer and a seller to carry out an NFT transaction, including the blockchain operators and not just the NFT marketplace.

Secondly, at no point during the transaction does the NFT marketplace have access to the sale consideration of the NFT. This non-custodial feature results in a situation of impossibility where the marketplace would have to pay 2% of the entire consideration, even when it does not have access to the consideration amount.

Thirdly, it is unclear whether the gas fees, which goes neither to the seller nor the e-commerce operator but directly to blockchain miners, would be considered to be part of the tax base for levy of EL in the hands of the NFT marketplace. Fourthly, it may be impractical or unfeasible for the e-commerce operator to keep track of the IP address or the location or residency of each buyer or seller for determining applicability of EL.

Withholding Tax

Section 194-O of the Income-tax Act, 1961 **("ITA")** imposes withholding tax obligations on e-commerce operator from April 1, 2020. Section 194-O provides that the e-commerce operator would be liable to withhold tax at the time of credit of consideration to the resident seller, at the rate of 1% of the gross amount of sale. Further, in case the sale is facilitated by the e-commerce operator, but payment is made by the buyer directly to the resident seller, section 194-O deems the e-commerce operator to have paid the resident seller such money and therefore be obligated to withhold income-tax at 1% on such sums as well. Section 194-O does not make a distinction between a resident and a non-resident e-commerce operator.

Therefore, basis a strict reading, the withholding obligations under section 194-O may also apply to a non-resident e-commerce operator facilitating sale of goods or provision of service of a resident seller, hence, increasing the compliance burden for non-resident e-commerce operators. Therefore, it may be possible that even though the non-custodial NFT marketplace does not credit the amount to the seller, it would be liable to deduct tax on the consideration paid directly to the seller through the smart contract. The application of this section would create cashflow problems for an NFT marketplace or similar facilitation platforms as they would have to withhold tax on gross consideration (including sales commission) irrespective of whether the consideration flows through them or not.

Tax Collection at Source

The buyer and the seller also need to discharge tax liability at the time of sale of goods. Section 206C imposes an obligation on a seller to collect tax at source **("TCS")** at rate of 0.1% of the sale consideration received on sale of goods in excess of INR 50 lacs as income-tax.[62] Please note that this tax is required to be collected by the seller from the buyer only if the total sales, gross receipts or turnover of the business carried on by the seller is more than INR 10 crores during the financial year immediately preceding the financial year in which the sale of goods is carried out.

Further, the TCS is deemed to be payment of tax on behalf of the buyer and the buyer is given the credit of such TCS.

Under the recently introduced section 194Q,[63] the buyer has a liability to deduct tax at source at a rate of 0.1% on the consideration paid for a sale or aggregate of sales exceeding INR 50 lacs, provided the buyer had a gross turnover exceeding INR 10 crores in the previous year. The interplay of section 206C and section 194Q is such that while section 206C releases the seller from the TCS liability if the buyer is required to withhold tax under any provision of the ITA, section 194Q to the contrary provides that the withholding obligation will be applicable on the buyer irrespective of seller's TCS liability.

Whereas in a physical sale of goods, a buyer and a seller could communicate to each other to figure out which provision would be applicable, such communication is limited when the sale of goods is taking place through an NFT transaction. Another concern for buyers is that when a sale of physical goods takes place through an NFT, either the seller or the marketplace would have to take responsibility for the delivery of the goods. This responsibility may not be currently accounted for in the terms of service of various marketplaces, as the focus is primarily on online sale of digital goods which could take place in a non-custodial manner through the operation of smart contracts.

Goods and Service Tax

Under the Goods and Services Tax **("GST")** regime, an NFT marketplace may be considered an intermediary. NFT marketplaces should ensure that they clearly demarcate the various fees and consideration amounts that are to be paid by the buyer, so that their liability for intermediary services is limited only to the extent of their sales commission.

Further, classification of the supplies for GST purposes would again depend on the nature of the underlying transaction. GST applicability would also depend on whether the NFT platform is located in India or outside. The GST regime also obligates electronic commerce operator to collect tax at source at a specified rate of the net value taxable supplies made through it by other suppliers where the consideration with respect to such supplies is to be collected by the operator.[64] In this regard, while the TCS obligation under GST may apply on normal marketplace wherein the consideration for supply is collected by the marketplace, in case of an NFT marketplace, the TCS obligation under GST should not apply as the consideration for supply is not collected by the NFT marketplace and is instead directly paid between parties through an automated contract.

62 Section 206C(1H) of the ITA; the provision comes into effect from October 1, 2020.

63 With effect from July 1, 2021.

64 Section 52 of the CGST Act, 2017.

While, the regulatory framework for blockchain and crypto-asset ecosystem is in limbo in India, it is essential that parties undertaking NFT transactions should correctly assess and comply with the tax obligations as applicable. Failure to do so may entail consequence for buyers, sellers or the marketplace as well.

— Ipsita Agarwalla & Meyyappan Nagappan

About NDA

At Nishith Desai Associates, we have earned the reputation of being Asia's most Innovative Law Firm — and the go-to specialists for companies around the world, looking to conduct businesses in India and for Indian companies considering business expansion abroad. In fact, we have conceptualized and created a state-of-the-art Blue Sky Thinking and Research Campus, Imaginarium Aligunjan, an international institution dedicated to designing a premeditated future with an embedded strategic foresight capability.

We are a research and strategy driven international firm with offices in Mumbai, Palo Alto (Silicon Valley), Bengaluru, Singapore, New Delhi, and New York. Our team comprises of specialists who provide strategic advice on legal, regulatory, and tax related matters in an integrated manner basis key insights carefully culled from the allied industries.

As an active participant in shaping India's regulatory environment, we at NDA, have the expertise and more importantly — the VISION — to navigate its complexities. Our ongoing endeavors in conducting and facilitating original research in emerging areas of law has helped us develop unparalleled proficiency to anticipate legal obstacles, mitigate potential risks and identify new opportunities for our clients on a global scale. Simply put, for conglomerates looking to conduct business in the subcontinent, NDA takes the uncertainty out of new frontiers.

As a firm of doyens, we pride ourselves in working with select clients within select verticals on complex matters. Our forte lies in providing innovative and strategic advice in futuristic areas of law such as those relating to Blockchain and virtual currencies, Internet of Things (IOT), Aviation, Artificial Intelligence, Privatization of Outer Space, Drones, Robotics, Virtual Reality, Ed-Tech, Med-Tech and Medical Devices and Nanotechnology with our key clientele comprising of marquee Fortune 500 corporations.

The firm has been consistently ranked as one of the Most Innovative Law Firms, across the globe. In fact, NDA has been the proud recipient of the Financial Times–RSG award 4 times in a row, (2014-2017) as the Most Innovative Indian Law Firm.

We are a trust based, non-hierarchical, democratic organization that leverages research and knowledge to deliver extraordinary value to our clients. Datum, our unique employer proposition has been developed into a global case study, aptly titled 'Management by Trust in a Democratic Enterprise,' published by John Wiley & Sons, USA.

Research@NDA

Research is the DNA of NDA. In early 1980s, our firm emerged from an extensive, and then pioneering, research by Nishith M. Desai on the taxation of cross-border transactions. The research book written by him provided the foundation for our international tax practice. Since then, we have relied upon research to be the cornerstone of our practice development. Today, research is fully ingrained in the firm's culture.

Over the years, we have produced some outstanding research papers, reports and articles. Almost on a daily basis, we analyze and offer our perspective on latest legal developments through our "Hotlines". These Hotlines provide immediate awareness and quick reference, and have been eagerly received. We also provide expanded commentary on issues through detailed articles for publication in newspapers and periodicals for dissemination to wider audience. Our NDA Labs dissect and analyze a published, distinctive legal transaction using multiple lenses and offer various perspectives, including some even overlooked by the executors of the transaction. We regularly write extensive research papers and disseminate them through our website. Our ThinkTank discourses on Taxation of eCommerce, Arbitration, and Direct Tax Code have been widely acknowledged.

As we continue to grow through our research-based approach, we now have established an exclusive four-acre, state-of-the-art research center, just a 45-minute ferry ride from Mumbai but in the middle of verdant hills of reclusive Alibaug-Raigadh district. Imaginarium AliGunjan is a platform for creative thinking; an apolitical ecosystem that connects multi-disciplinary threads of ideas, innovation and imagination. Designed to inspire 'blue sky' thinking, research, exploration and synthesis, reflections and communication, it aims to bring in wholeness — that leads to answers to the biggest challenges of our time and beyond. It seeks to be a bridge that connects the futuristic advancements of diverse disciplines. It offers a space, both virtually and literally, for integration and synthesis of knowhow and innovation from various streams and serves as a dais to internationally renowned professionals to share their expertise and experience with our associates and select clients.

We would love to hear from you about any suggestions you may have on our research publications. Please feel free to contact us at **research@nishithdesai.com**.

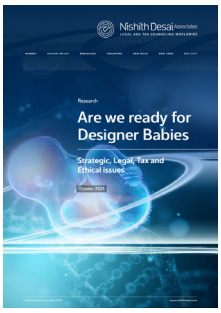
Recent Research Papers

Extensive knowledge gained through our original research is a source of our expertise.

October 2024

Unmasking Deepfakes

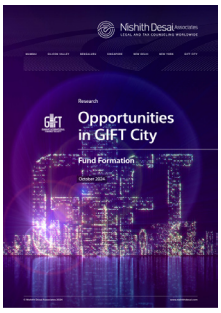
Legal, Regulatory and Ethical Considerations



October 2024

Are we ready for Designer Babies

Strategic, Legal, Tax and Ethical issues



October

Opportunities in GIFT City

Fund Formation

August 2024

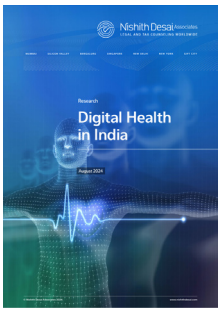
Telemedicine in India

The Future of Medical Practice

August 2024

Clinical Trials and Biomedical Research in India

Legal and Regulatory Framework



August 2024

Digital Health in India

For more research papers **click here**.

Nishith Desai Associates

LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI

93 B, Mittal Court, Nariman Point
Mumbai 400 021, India

Tel +91 22 6669 5000

SILICON VALLEY

220 S California Ave., Suite 201
Palo Alto, California 94306, USA

Tel +1 650 325 7100

BENGALURU

Prestige Loka, G01, 7/1 Brunton Rd
Bengaluru 560 025, India

Tel +91 80 6693 5000

SINGAPORE

Level 24, CapitaGreen
138 Market St
Singapore 048 946

Tel +65 6550 9855

MUMBAI BKC

3, North Avenue, Maker Maxity
Bandra–Kurla Complex
Mumbai 400 051, India

Tel +91 22 6159 5000

NEW DELHI

13-H, Hansalaya Building, 15
Barakhamba Road, Connaught Place
New Delhi 110 001, India

Tel +91 11 4906 5000

NEW YORK

1185 6th Avenue, Suite 326
New York, NY 10036, USA

Tel +1 212 464 7050

GIFT CITY

408, 4th Floor, Pragya Towers
GIFT City, Gandhinagar
Gujarat 382 355, India

Fintech

Legal, Regulatory and Tax Considerations – Compendium

concierge@nishithdesai.com