Rajeshwar Rao: Open banking in India

Remarks by Mr Rajeshwar Rao, Deputy Governor of the Reserve Bank of India, in a webinar on Open Banking, organised by Tata Consultancy Services (TCS) in association with the Embassy of India in Brazil, 14 April 2021.

* * *

Ladies and Gentlemen,

A very warm good morning to you in Brasilia with the hopes and prayers that all of you remain safe and healthy from the clutches of the pandemic that is still raging amongst us. I am grateful to His Excellency, Shri Suresh Reddy, Ambassador of India in Brazil for extending this kind invitation to interact with you all in this futuristic but extremely relevant topic of Open Banking[1].

1. The modern world has become increasingly interconnected with mobile phones and handheld devices with internet connection enabling ubiquitous access and broader reach to information, services, and products. While technology is the omnipresent enabler in all modern human endeavours, it harnesses a disruptive power challenging the well-proven business models, opening new markets, while blurring the boundaries of geographical segmentation.

2. Technology has enabled and indeed empowered banks and financial firms to penetrate hitherto untouched market segments which have remained beyond the reach of formal financial systems and players despite significant progress in financial delivery methods. In the recent years, technology driven modes of financing, new financial business models, specialized financial services and products are emerging and driving FinTech innovation in areas such as P2P lending, wealth management, microfinance, smart-contract, AI/ML based decision analysis systems and robo-advisory, etc. and have started to shape the regulatory engagements and discourse. Integral to this discourse are the issues concerning data sharing, data access and to a large extent data democratisation.

3. The financial plumbing that once extensively focused on payments channels and transactions, now also looks to accessing the financial data of consumers. Digital exchange of financial data can become the building block for new emerging service models, removing inefficiencies in the system and opening new product possibilities. Therefore, regulators and national authorities are beginning to acknowledge the fact that enabling a simplified framework for financial information data exchange has the potential to transform the financial systems and may lead to product innovation and better facilitation of financial services for customers and end-users. Therefore, the financial data access and distribution has significant implications not only for the concerned stakeholder institutions but also for future economic growth.

4. An individual's financial data is normally fragmented and spread across in the silos of data warehouses of financial institutions, government bodies and in some cases regulators. Though there exists some sort of formalised frameworks for seamless, safe, and swift data sharing between financial information providers (FIPs) and financial information users (FIUs), there still exists a void in terms of legally enforceable and permitted integrated solutions to aggregate user data for a seamless, wide-ranging picture of the financial history and transactions of the individuals and firms. Consequently, this vast amount of fragmented information is not being effectively optimised to identify and address financial needs and provide comprehensive service delivery to end-users.

5. In this regard, a BCBS study report[2] has observed that while sharing of bank-held, customer-permissioned data with third parties has been taking place for several years, increased use of digital devices and rapidly advancing data aggregation techniques are transforming retail banking services across the globe. This sharing of customer-permissioned data by banks with third

parties is leveraged to build applications and services that provide faster and easier payments, greater financial transparency and options for account holders, new and improved account services, as well as additional marketing and cross-selling opportunities.

6. Such initiatives also raise the issue of whether financial institutions as holders of data of individual customers should act only as agents and whether they should have ownership stake driven by commercial considerations. It is quite clear that the right to data accessibility and usage should vest in the owners of data rather than the holders of data. Apart from this data democratisation, there are major concerns around transportation and storage of data in safe and secured manner enveloped within a consent-based architecture. Different jurisdictions are currently trying to address this need for a framework that allows efficient and secure navigation and enables use of customer's financial data through different methods; for example, by allowing use of open API frameworks within financial institution's user applications. In India, we too have envisioned a similar ecosystem of account aggregators (AAs) to broaden the scope of financial data sharing.

Let me dwell briefly on the Indian context:

Open Banking Initiatives in India

7. Globally, open banking regulatory frameworks are structured to enable third party access to customer-permissioned data, requiring licencing or authorisation of third parties, and implementing data privacy and disclosure and consent requirements. Some frameworks may also contain provisions related to whether third parties can share and/or resell data onward to "fourth parties", use the data for purposes beyond the customer's original consent and to whether banks or third parties could be remunerated for sharing data. Open banking frameworks may also contain expectations or requirements on data storage and security.

8. India has kickstarted its approach to Open Banking by enabling an intermediary which will be responsible for the customers' consent management. These intermediaries are licensed as Non-Banking Financial Companies. In September 2016, RBI announced creation of a new licensed entity called Account Aggregator (AA) and allowed them to consolidate financial information of a customer held with different financial entities, spread across financial sector regulators. In India, AA acts as an intermediary between Financial Information Provider (FIP) such as bank, banking company, non-banking financial company, asset management company, depository, depository participant, insurance company, insurance repository, pension fund etc., and Financial Information User (FIU) which are entities registered with and regulated by any financial sector regulator. The flow of information takes place through appropriate Application Programming Interfaces (APIs).

9. The transfer of such information is based on an explicit consent of the customer and with appropriate agreements/ authorisations between the AA, the customer, and the financial information providers. Data cannot be stored by the aggregator or used by it for any other purpose. Explicit and robust data security and customer grievance redressal mechanisms have been prescribed and the Account Aggregators are not permitted to undertake any other activity, primarily to protect the customers' interest.

Consent based architecture

10. The emphasis of regulatory framework for account aggregators in India is thus on explicit customer consent for data sharing. No financial information of the customer is to be retrieved, shared, or transferred without the explicit consent of the customer. The other tenets of this open banking initiatives in India are – financial data integrity, security & confidentiality, robust IT governance & controls, and strong customer protection & grievance redressal mechanism. Further, in order to facilitate seamless movement of data & consent-based sharing of financial information in the AA ecosystem, a set of core technical specifications have been framed by

Reserve Bank Information Technology Private Limited (ReBIT), a wholly-owned subsidiary of the RBI for adoption by all regulated entities, acting either as Financial Information Providers (FIP) or Financial Information Users (FIU) in November 2019.

11. In order to protect critical financial information of users and to enforce a mechanism for obtaining proper consent from customers, the consent of the customer to be obtained by the Account Aggregator shall be a standardised electronic consent format as prescribed under regulations. The AA is required to inform the customer of all necessary attributes to be contained in the consent format and the rights of the customer to file complaints. The customers are also provided a functionality to revoke consent post which a fresh consent would have to be obtained. Explicit onus has also been placed on Financial Information provider (FIP) to verify – validity of the consent, specified date and usage of it and the credentials of the AA.

12. Different jurisdictions have taken a different approach on the issue of Open Banking. While some have adopted a prescriptive approach, requiring banks to share customer-permissioned data and requiring third party users to register with regulatory authorities, others have taken a facilitative approach by issuing guidance and recommended standards, and releasing open API standards and technical specifications. Some jurisdictions also appear to be following a market-driven approach, currently having no explicit rules or guidance.

13. The AA is a regulatory initiative in India under a hybrid model which is a combination of prescriptive & facilitative approaches and is in its early stages of development. One of the key things to look out for is whether the market forces will drive the adoption of this initiative or further regulatory nudge will be required. The pace of adoption will also depend on the strength of the community to come together and continue to drive the technical specifications standards and scalability potential.

Now, to continue with the tradition of a central banker and regulator, let me also enunciate few risks and spread some words of caution along the way.

Risks associated with Open Banking

14. Open banking may offer benefits in the form of convenient access to financial data and services to consumers and streamlining some costs for financial institutions. However, it also potentially poses significant risks and concerns around:

- Financial privacy and data security: In open banking frameworks, risks associated with the loss or theft of personal data on account of poor security, data protection violations, money laundering, and terrorist financing concerns cannot be ruled out. Therefore, large scale adoption of open banking frameworks should ideally be preceded by strong data protection and privacy laws. Such laws should anchor the ownership rights and ensure control and consent-based use of the data. They should also establish the boundaries of rights and obligations of third-party use, down-streaming of data to fourth parties and reselling it. India has already embarked upon the same and The Personal Data Protection Bill, 2019 has already been introduced. The Bill seeks to provide for protection of personal data of individuals and establishes a Data Protection Authority for the same.

- Customer liability: In absence of explicit arrangements for redressal of customer grievances and limiting their liability in case of erroneous or fraudulent activity, the acceptability of open banking frameworks may remain limited. Therefore, the jurisdictions should look to address customer liability for third party access of data through customer protection or indemnity laws. RBI has issued Charter of Customer Rights in December 2014 which lists ‘right to privacy’ along with ‘right to grievance redress and compensation’ among others. The right to privacy requires that customers’ personal information should be kept confidential unless they have offered specific consent to the financial services provider or such information is required to be provided under the law or it is provided for a mandated business purpose.

- Cybersecurity and Operational Risks: Use of open banking architectures, which is premised on the enhanced sharing of data, increases the surface area for cyber frauds. As the open API provides uncluttered access to customer banking data such as transactions and balance stored within the infrastructure, it may also pose a severe cybersecurity risk. Losses caused to customers on account of cyber events would require financial institutions to compensate customers for such losses. Institutions may also face a variety of potential operational and cyber security issues related to the use of APIs, including data breaches, misuse, falsification, denial of service attacks and infrastructure malfunction.

- Compliance and Reputational Risk: While open banking expands vistas of traditional banking and offers unique business opportunities, it also reposes extreme responsibilities with respect to compliance with applicable prudential regulations and privacy laws. Risks arise due to exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements due to omissions and commissions of the third-party service provider.

- Grievance Redressal: With more parties and intermediaries involved in the provision of financial services in an open banking model, it is more difficult to assign liability. If the regulations governing customer grievance redressals are not updated to take open banking business models into consideration, the national authorities may find it difficult to provide the customers adequate levels of protections. In India, RBI has implemented a separate Ombudsman Scheme for Digital Transactions in January 2019. The number of complaints received under the Ombudsman Scheme for Digital Transactions (OSDT) have been consistently increasing reflecting increased adoption of digital modes of banking.

15. In addition to the above, open banking frameworks also present regulators with many challenges. In open banking, there can be wide-ranging third-party arrangements such as fintech firms, intermediary firms engaged in data aggregation and other service providers which may not have a contractual agreement with the bank over which regulators can exercise jurisdiction. Further, it may be possible that several of these firms may not fall under regulatory purview of any financial sector regulator. In such situations, it may become difficult for regulators to set requirements, specifications, and exercise regulatory jurisprudence.

16. In many jurisdictions, including India, outsourcing arrangements for banks and other regulated entities are covered under explicit regulations. Supervisors also have certain amount of oversight over the third-party entities. If the relationships in the open banking extend beyond the existing supervisory and regulatory perimeters, the enforcement of standards and prudential policies may become difficult.

Conclusion

17. Open banking is a potential disruptor in financial system and may change the way of doing banking for both- customers and banks. New pure tech-play entities have the potential to snatch market share from established but traditional financial institutions because they are technologically more advanced, digitally agile to cater to customer needs with higher efficiency, have better user interface, and are more competitive in pricing.

18. In contrast to the Open Banking initiatives witnessed in some countries, India has embraced an approach where both the Regulator and the market have collaborated for the development of the Open Banking space. In India, RBI and NPCI came out with a payment system like UPI and released its API for the banks and third-party app providers to build upon. The market participants are also driving innovation and many banks are releasing their own APIs and joining forces with the fintech companies to provide better experience to their customers. Moreover, with the launch of Regulatory Sandbox and Reserve Bank Innovation Hub, RBI's approach has been that of encouragement and guidance.

19. At the same time, all stakeholders need to appreciate the fact that while technological innovation is of paramount importance, the customer privacy and data protection are non-negotiable. We must generate trust amongst the customers that their data is safe and secure in all their financial relationships with regulated entities and for that – innovation and regulation should go hand-in-hand. Regulators and Supervisors should also gear-up for the future challenges. Afterall, as the saying goes for (Regulators)….. "while they can overlook the weather of the day, they cannot ignore climate of the era".

Thank you.

---

[1] Open banking is defined as the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services, including for example those that provide real-time payments, greater financial transparency options for account holders, marketing and cross-selling opportunities. Individual jurisdictions may define open banking differently (BCBS; November 2019).

[2] November 2019; Report on open banking and application programming interfaces; Basel Committee on Banking Supervision; Bank for International Settlements