RECONCILING THE ACCOUNT AGGREGATOR AND CONSENT MANAGER FRAMEWORKS

Evolution of the AA Framework

The foundation of the AA framework can be traced back to the recommendations of the Financial Sector Legislative Reforms Commission ("**FSLRC**") in 2013, which highlighted the need for a more integrated and efficient financial system in India. In 2016, the Reserve Bank of India ("**RBI**") introduced the AA Master Directions which established the regulatory groundwork for AAs. The subsequent introduction of the Data Empowerment and Protection Architecture ("**DEPA**") in 2020 further strengthened this by enabling secure and user-consented data sharing, ensuring individuals have greater control over their financial data.

Prior to the introduction of the AA framework, the sharing of financial data was not regulated through a secure framework. SMS-scraping and screen-scraping were popular modes for financial entities to obtain relevant information. Alternatively, customers were required to give physical or digital documentation to individual representatives. This posed significant risks as data was being shared through unsecure modes and/or data transmission protocols without the explicit consent of customers. Further, customers were largely unaware of the relevance of the personal data usage by companies and consents given by them, which were almost always captured in lengthy legal documents or terms of service. This is in sharp contrast with the AA framework, which emphasises user autonomy, explicit consent, and data security through encryption and specific purpose codes.

An AA is "*a non-banking financial company… that undertakes the business of an account aggregator, for a fee or otherwise...".* A key aspect to note is that the 'business of an account aggregator' means the "*business of providing under a contract, the service of, retrieving or collecting such financial information pertaining to its customer, as may be specified by the RBI from time to time; and consolidating, organizing and presenting such information to the customer or any other financial information user as may be specified by the RBI*." Further, the AA Master Directions entrust AAs to perform "*the function of obtaining, submitting and managing the customer's consent*".

In other words, AAs are RBI-regulated entities that perform the function of sharing financial data based on the explicit consent of the customer for such sharing of financial information between regulated entities called Financial Information Providers ("**FIPs**") and Financial Information Users ("**FIUs**"). AAs perform three major functions — (a) enabling customers to manage their consent in relation to the retrieval and sharing of their financial data, (b) retrieving such financial information from FIPs and sharing it with FIUs, and (c) consolidating and presenting such information to customers. Thus, AAs, by virtue of their operations, have been acting as the Consent Managers for financial data, in accordance with the AA Master Directions.

Today, there are 16 NBFC-AAs with an operational licence from the RBI and another 2 NBFC-AAs with an in-principle licence from the RBI. The AA ecosystem, which is predicated on *explicit consent* of the customer, is a Digital Public Infrastructure (DPI) operating at scale. A few key points:

- More than 600 financial institutions (regulated entities) participate in the AA framework, including large public and private financial institutions regulated by the Reserve Bank of India, Securities and Exchange Board of India, Insurance Regulatory and Development Authority of India and Pension Fund Regulatory and Development Authority.
- With all large financial institutions joining the AA framework, around 60% of the financial accounts (2.12 billion out of more than 3.5 billion financial accounts) of the country have the facility of sharing data and managing consents using AAs.
- 16 financial information types can be shared via the AAs.
- More than 140 million consent requests have been successfully fulfilled using AAs as of December 2024 and it is estimated that almost 7-8% of the Indian population has already registered with AAs to give and manage their consents for sharing financial data.
- The AA ecosystem is rapidly growing at a month-on-month growth rate of 13% in relation to cumulative consent requests.
- The entire AA framework is based on open standards and APIs which allow population-scale implementation, designed for competition amongst Consent Managers, and enable easy technical interoperability.

Similarities between the AA and CM frameworks

In essence, consent management within the AA framework is a *means to the end* of secure, consent-driven financial data sharing. A CM, on the other hand, is primarily tasked with the function of consent management for individuals in relation to processing of all kinds of personal data by data fiduciaries, with sharing of such personal data with data fiduciaries being an ancillary function that CMs may choose to enable. Thus, consent management and data sharing are functions enabled by AAs as well as CMs.

It is also important to note that data-blindness, restrictions on outsourcing, net worth requirements, facilitating data principal rights, implementing strong data security measures such as encryption and maintenance of logs, etc. are related obligations that both entities are required to undertake under their respective frameworks. Additionally, an AA is required to seek prior approval of the RBI in case of change of control (whereby a change of control is defined as the acquisition of more than 26% of shareholding), whereas the Draft Rules also require CMs to obtain prior approval of the Data Protection Board of India ("**the Board**") for any change in control. We would like to highlight that both the AAs and CMs are ultimately required to protect customers' interests. Specifically, an AA is required to publish a citizen's charter which elucidates on a customer's rights in relation to their personal data. Similarly, CMs have an obligation under the Draft Rules to act in a fiduciary capacity in relation to the data principal. This showcases that both frameworks are inherently designed to protect and preserve customer rights and autonomy.

Reconciling the AA and CM Frameworks

While MeitY's efforts to clarify the registration and other obligations of Consent Managers are indeed laudable, we have proposed a few revisions which may be incorporated to the Draft Rules, which would help provide clarity and ensure the continuity of existing sector-specific regulatory

frameworks. This will also provide for effective implementation of the CM framework under the DPDPA.

1. CLARIFY THAT REGISTRATION AS CONSENT MANAGER IS MANDATORY

Section 6(9) of the DPDPA provides that, "*every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed*". However, the current framing of Rule 4(1) of the Draft Rules suggests that applying for such registration may be optional.[1]

In our understanding, the intention of the DPDPA regime is to ensure that all entities engaging in the business of consent management must be duly registered with the Board. To ensure clarity, we recommend appropriate amendments in Rule 4(1).

2. ALLOW REGISTRATION OF SECTOR-SPECIFIC CONSENT MANAGERS OPERATING UNDER SECTORAL REGULATIONS

The MeitY should take note of existing sector-specific regulatory frameworks which set out registration and other requirements for performing the functions of a consent manager. In order to ensure that the Consent Manager ecosystem under the DPDPA takes flight and gets implemented at population scale, it would be appropriate to create an enabling framework for cross-registration of sector-specific entities performing functions of a Consent Manager under extant laws.

- **Financial data** - In order to perform the functions of a Consent Manager by enabling collection of consent and consequent sharing of financial data across Data Fiduciaries (similar to Item 2 of, Part B, First Schedule to the Draft Rules), it is mandatory to hold a valid NBFC-AA licence as per the AA Master Directions. Notably, the AA Master Directions limit the operations of AAs to only the financial data types defined therein, and to onboard only such entities which are registered and regulated by any of the financial sector regulators, i.e. FIUs and FIPs. As a corollary, in the context of financial data, a reasonable and harmonious construction of regulatory and statutory requirements would require entities holding a valid NBFC-AA licence to also be registered as Consent Managers under the DPDPA.

- **Health data** - The Financial Health Records (FHR) framework under the National Health Authority (NHA) is in advanced stages of its sandbox, with an extensive framework of

[1] *4. Registration and obligations of Consent Manager. – (1) A person who fulfils the conditions of registration of Consent Managers in Part A of First Schedule <u>may</u> apply to the Board for registration as a Consent Manager …" (Emphasis supplied)*

the consent artefact and data schema for health data[2]. A similar sectoral approach of registering Consent Managers approved by the NHA for the healthcare sector as Consent Managers under the DPDPA would ensure continuity and smooth implementation of the Consent Manager framework for the healthcare sector.

Moreover, in the context of the existing sector-specific regulatory frameworks for consent management[3], we recommend that the MeitY consider permitting entities already engaged in performing the functions of a CM under applicable sector-specific regulatory frameworks, to operate as Consent Managers. Further, the Rules may empower the Board to **provide appropriate exemptions/concessions** to such entities for the period between setting up of the Board and the commencement of the process of registration of Consent Managers under the DPDPA, to operate as Consent Managers.

AAs would make the perfect case for this exemption since they are already registered and regulated under the AA Master Directions. Simplifying the registration process and requirements for AAs and such other entities would **avoid duplicity** and also benefit from the strict scrutiny already undertaken by the relevant sectoral regulators. Accordingly, we propose inclusion of an appropriate *proviso* to be added to Rule 4(1)[4].

3. CLARIFY MODE OF INSTRUCTION & DATA SHARING THROUGH CM

In our understanding, Illustration 2 in Part B of First Schedule is meant to describe a process whereby the data principal instructs their bank (B2) through the platform of the Consent Manager to share their bank statement with B1. We recommend a minor amendment to the said illustration to clarify this and avoid any contrary suggestions about the instruction being made outside the platform.

4. CLARIFY CONFLICT OF INTEREST CLAUSE FOR CMs

Items 9 and 10 of Part B of First Schedule to the Draft Rules requires Consent Managers to have measures to ensure that no conflict of interest arises on account of its directors, key managerial personnel and senior management having a directorship, financial interest, employment or beneficial ownership in data fiduciaries, or having a material pecuniary relationship with them.

---

[2] Health Repository APIs - https://sandbox.abdm.gov.in/sandbox/v3/documentation?doc=apis;
Health Data Consent Manager (HDCM) APIs -
https://sandbox.abdm.gov.in/sandbox/v3/documentation?doc=cm_gateway;
Purpose codes and Health Information (HI) types -
https://sandbox.abdm.gov.in/sandbox/v3/documentation?doc=apis;
Fast Healthcare Interoperability Resources (FHIR) schema for electronic health records -
https://www.nrces.in/ndhm/fhir/r4/index.html and https://www.nrces.in/ndhm/fhir/r4/profiles.html

[3] The Ministry of Agriculture and Farmer Welfare has also been actively developing the Agri Stack framework, which seeks to empower farmers to be able to share their agricultural data, based on their consent.

[4] A similar proviso is also included by the RBI in the AA Master Directions.

From our experiences in the AA ecosystem, it is relevant to note that setting up of viable business models would inevitably require AAs or CMs to enter into appropriate commercial arrangements with data fiduciaries for provision of services on their platform (apart from potential customer facing revenue models). Such commercial arrangements should not, by themselves, be construed as a conflict of interest.

Notably, in other regulated sectors where intermediate entities are required to act in the best interests of the customer, they are permitted to engage in commercial arrangements with the manufacturers/ service providers. For instance, while Insurance Brokers are required to act in the best interests of the client (end customer), commercial engagements with insurance manufacturers are permitted as a business model.[5] Further, a Consent Manager provides a valuable service to the data fiduciaries which it onboards onto its platform – for which, it should be entitled to have appropriate commercial arrangements with such data fiduciaries.

Various regulatory and market factors can counter apparent or perceived conflicts of interest because of such commercial arrangements. Several regulators have deployed frameworks that ensure that the intermediaries represent and work in the best interests of the customers. A few facets of such frameworks include:

a. Existing prohibitions on conflict of interest of directors, key managerial personnel and senior management: These restrictions would address the most significant and tangible form of conflict of interest between a CM and a data fiduciary.
b. Clarity in charter and codes of conduct: The charter of the entities must demonstrate a strong commitment to the customers. This can be bolstered by codes of conduct issued by industry bodies, such as the Insurance Brokers Association of India (IBAI) for insurance brokers.[6]
c. Strong supervisory and regulatory oversights: Any residual concerns regarding conflict of interests between CMs and data fiduciaries are more appropriately addressed by requiring strong governance and audit practices from the CMs. These can be in the form of strict customer grievance redressal procedures, coupled with close regulatory oversight over the entities, which in this case would come under the ambit of the Data Protection Board.
d. Market Factors: In a relationship of this nature, customers will eventually reject intermediaries (Consent Managers) which fail to act in the best interests of the

---

[5] Clause 1, Schedule I - Form H, Code of Conduct, IRDAI (Insurance Brokers) Regulations, 2018:
"*Insurance Brokers, Every insurance broker shall follow recognised standards of professional conduct and discharge their functions in the interest of the clients or policyholders*.";
Clause 2, Schedule I - Form H, Code of Conduct, IRDAI (Insurance Brokers) Regulations, 2018:
"*Conduct in matters relating to clients relationship— Every insurance broker shall:*
(a) conduct its dealings with clients with utmost good faith and integrity at all times;
(b) act with care and diligence; …"

[6] IBAI Code of Conduct, available at
https://www.ibai.org/storage/media/news_letter/ibai-code-of-conduct_24012024-120814.pdf
"***Act in the best interests of each client.***
Act in a manner which pays due regard to the best interests of each client and ensure decisions and recommendations are based on a clear understanding of their needs, priorities, concerns and circumstances."

customer and the market would auto-align to retain only those entities which protect customer interests.

Thus, allowing Consent Managers to have commercial arrangements with Data Fiduciaries seeking to onboard on the CM's platform would not pose a tangible conflict of interest on account of the above factors. In fact, it would extend much needed clarity to businesses on the scope of permitted operations of a Consent Manager, and help them to appropriately structure their business models to ensure long term viability and success of the consent manager ecosystem.

It is pertinent to note that in the Account Aggregator ecosystem, all AAs have operating business models wherein the customers do not have to take the burden of fees for availing the services of AAs. Rather, the FIUs pay AAs based on the number of data fetches made by them. One rationale behind the approach has also been to encourage customers to adopt and get access to this data empowerment and protection framework without any monetary implications or barriers for them. This has been a proven approach used by the industry, regulators and policymakers for promoting essential products and services such as insurance and consented data sharing facilities via the AA Framework. The AA Master Directions require AAs to have a transparent pricing mechanism.[7] This addresses any perceived conflict of interest by disincentivising more data fetches than is necessary for the underlying purpose. In addition, the AA Master Directions also ensure that AAs act in the best interests of customers by obligating AAs to have a citizens charter explicitly guaranteeing protection of customer rights.[8]

In this context, it would be helpful to suitably include a proviso to Items 9 and 10 to clarify that commercial arrangements with data fiduciaries for provision of services as a Consent Manager shall not, by itself, be construed as a conflict of interest.

5. GRIEVANCE REDRESSAL AND APPEALS

The AA Master Directions and the DPDPA read with the Draft Rules are designed to protect customers' rights. Both frameworks require publishing of a policy on the timelines for resolution of grievances received, as well as the details of the grievance officer. To this extent, both frameworks are aligned.

---

[7] Clause 13, AA Master Directions
"***13. Pricing***
13.1 An Account Aggregator would require to have a Board approved policy for pricing of services. Pricing of services will be in strict conformity with the internal guidelines adopted by the Account Aggregator which need to be transparent and available in public domain."

[8] Clause 5(j), AA Master Directions
"***5. Duties and Responsibilities of an Account Aggregator***

(j) Account Aggregator shall have a Citizen's Charter that explicitly guarantees protection of the rights of a customer. The Account Aggregator shall not part with any information that it may come to acquire from/ on behalf of a customer without the explicit consent of the customer."

It would however remain to be adjudged where an appropriate appeal lies. Under the AA Master Directions, an appeal may be preferred to the RBI, including through the RBI's ombudsman scheme. However, under the DPDPA, recourse against Consent Managers would lie with the Board and the Telecom Disputes Settlement and Appellate Tribunal ("**TDSAT**"). In this context, it is important to note that the recourse under the AA Master Directions is broader as it provides for recourse to file an appeal by all *customers*, and is not limited to natural persons, unlike the DPDPA which only provides recourse to a natural person.

To this extent, additional legal clarity would be important to streamline the appeal process. One potential way to harmonise the two frameworks could be based on a reading of Section 38 of the DPDPA – such that recourse to the Board could serve as an avenue for a data principal *in addition* to an appeal before the RBI. In other contexts of regulatory overlaps, there are judicial precedents stating that the relevant sectoral regulator, i.e., the RBI in this case, would take precedence over the subject matter regulator/adjudicator, i.e., the Board in this case. Such a reading would also ease the burden on the Board which may further investigate and make a determination based on the findings of the RBI in respect of a particular matter.[9] This interpretational clarity can be built over the course of time through the decisions of relevant fora and does not require any amendments in the Draft Rules per se.

6. INTEROPERABILITY

It is our understanding that references to interoperability in the context of Consent Managers in the DPDPA and the Draft Rules are in relation to the *technical* interoperability of Consent Managers with data fiduciaries through a standardised set of API implementations such that a Consent Manager has the *technical* capability to integrate with any data fiduciary, subject to any limitations on such integrations under applicable laws. Further, we understand that such technical aspects will be published by the Board.

We would deeply appreciate a line of confirmation from the MeitY on this aspect. If so, we would be keen to work closely with the Board in the development of the standards and assurance framework and share our learnings on similar aspects from the AA ecosystem, which has spent the last few years creating an effective base for technical standards for interoperability across regulated entities in the financial sector.

******

[9] In *Bharti Airtel v. CCI & Ors*., Supreme Court of India, Civil Appeal No. 11843 of 2018 (5 December 2018), the jurisdiction of the CCI was pushed to a later phase as TRAI had to decide certain factual issues first. The Supreme Court found that TRAI has the expertise to deal with the issues in the telecom sector that arise from the TRAI Act, 1997. The Supreme Court observed that TRAI is empowered to scrutinise the issue first and if there is evidence to prove that anti-competitive conduct exists, the jurisdiction of the CCI can be enforced.