Code of Conduct for Sahamati Members

Driven by discussions and decisions in Committees, User Councils and Working Groups facilitated by Sahamati.

June 11, 2025

Disclaimer

Nothing stated herein should be construed as legal advice in any manner. The views expressed in this document are based on outcomes of discussions conducted with stakeholders in relevant committee(s), user council(s) and/or working group(s) anchored by Sahamati and do not affect the requirements of any applicable provisions of law or the rules, regulations, guidelines, or circulars administered by the Reserve Bank of India, Securities and Exchange Board of India or any other relevant regulator or statutory body.

You are advised to seek independent legal opinion on the applicability of any applicable laws and/or regulations relevant to your specific circumstances.

Revision History

Version	Date	Changes Made
Version 1.0	August 31, 2022	First release for the AA Community
Version 1.1	December 02, 2023	Update to PC004 and PC001
Version 1.2	February 23, 2024	Structural changes to the documents: removed guidelines tagged "Under Deliberation" - CG003, CG004, CG005, UA002, UA003, UA004, AD001, AD005, AD006, AL004, CR002, CR005, CR006, CR007, CR008, CR010, CR011, CR012, DR001, DR002, DR004, CL002, CL003, RC001, RC002, RC003, RC004, CDR002, CDR003, CDR004, FUR002, FUR005, FUR006, FUR007, FPR003, R002, PC002, PC003, PC005, AC003, AC004, AC010, AC011, AAC001, AAC002, PT004, PT005, GD004, SL001, SL002, AI002, SD003, SD004, CF003
		Deprecated sections “Unregulated entities and their Roles” & “LSP Implementation.”
		Reindexed Code Numbers for Topics - “Customer registration and de-registration, Central Registry and Token Issuance Service”
		Updated to certain codes based on recent regulatory and policy changes - code nos. AD004, AD008, AL003, CR001, CR011, CR013, FUR001, FPR004, FPR005, FPR006, PC001, AC007, PT005
		Deprecated certain codes based on recent regulatory and policy changes - code nos. - UA004, AAC001, AI003, UR001, UR002, UR003, LSP001, LSP002, LSP003
		Added Code DR005
Version 2.0	June 11, 2025	● Included ‘Target Audience’ & ‘Treatment’ against each code of conduct. ● Deprecated the following codes, which no longer remain relevant: DR001, DR002, DR004, CF003, CF004, CR001, CR002, CR005, CR006, CR007, CR008, CR010, CR011, CR012, FUR001, FUR002, FPR003, FPR004, FPR005, FPR006, AC001, PT001, PT002, PT003, PT004, PT005, PT006, AD001, AD005, AD006, SD001, AI003, SD002 ● Revised numbering of codes

Version	Date	Changes Made
		- Added Code of Conduct nos.: CC008, CC009, CC027, CC028, CC029, CC030, CC031, CC032, CC033, CC034, CC039, CC040, CC053

Purpose of this document

The AA Master Directions issued by RBI and Technical Specifications published by ReBIT provide an overarching framework to guide dos and don'ts of Sahamati members and other regulated entities participating in the account aggregator (“**AA**”) ecosystem.

These codes of conduct address various ‘operational’ issues that arise while operating in the AA ecosystem, and provide clarity on issues of interpreting the above-mentioned high-level directions/specifications. These codes of conduct are crafted to operate as lower-level procedural decisions that are understood and implemented uniformly by Sahamati members and other regulated entities participating in the AA ecosystem.

Such “procedural decisions” are the product of community deliberations in one or more of the committee(s), user council(s) and/or working group(s) that Sahamati facilitates.

Once such procedural decisions are published in the form of code(s) of conduct, they are required to be adhered to by all Sahamati members and other regulated entities participating in the AA ecosystem, based on the treatment mentioned in such code(s) of conduct i.e. mandatory vs. recommendatory.

Such code(s) of conduct usually also make their way into the various checklists published by Sahamati to guide implementations and conduct of Sahamati members in the AA ecosystem.

Sahamati members and other participants in the AA ecosystem are expected to not proceed with divergent implementations. While market pressures motivate faster consensus on such matters, they should not be reasons for divergent behaviours, as that may be detrimental to end customers as well as the AA ecosystem at large.

Modifications to such code(s) of conduct, based on newer market feedback or regulatory guidance, are, of course, to be handled from time to time through further deliberations in the relevant committee(s), user council(s) and/or working group(s), if required.

This document aims to consolidate all code(s) of conduct (and their lifecycle stage) discussed thus far, across Sahamati’s committees, user councils and working groups.

Enforcement of Sahamati’s Codes of Conduct

Enforcement of adherence follows a three-step process:

- Clarity and explanation - through checklists circulated by Sahamati.
- Review of checklists and explanation of deviations - during onboarding assistance provided by Sahamati.

- Transparency of information pertaining to adherence - through public dashboards available on Sahamati's website.

Punitive measures to ensure enforcement of such guidelines are outside the scope of this document.

The overarching spirit of this document is to provide clarity to all Sahamati members and other regulated entities participating in the AA ecosystem on convergent thinking on various subjects. Such clarity is expected to foster adherence and healthy discussions amongst Sahamati members and other ecosystem participants. This document is intended to serve such an audience.

This document includes the 'Treatment' of each Code of Conduct as Mandatory, Recommended or Clarificatory, which should be understood as below:

A. **Mandatory** - This means that the code of conduct must be followed by all Sahamati Members. The general expectation from the community is that all participants adhere to these codes of conduct.

B. **Recommendatory** - This means that the code of conduct has been agreed by the broader community as a best practice for Sahamati Members and other participants.

C. **Clarificatory** - This means the code of conduct aims to clarify either an ambiguity arising from the relevant ReBIT specifications, or matters of general importance which should be consistently adopted by Sahamati Members and other participants.

How to read this document:

- If you are an FIU, please refer to Chapters I and II.
- If you are an AA, please refer to Chapters I and III.
- If you are an FIP, please refer to Chapters I and IV.

Online access to these Codes of Conduct

These codes of conduct are available on Sahamati's website at
https://sahamati.org.in/member-code-of-conduct/

Table of Contents

CHAPTER I

Common Codes of Conduct applicable to FIUs, AAs and FIPs

1. Central Registry and Token Issuance

Code of Conduct No.	CC001
Target audience	FIUs, AAs, FIPs
Purpose	To clarify the need for onboarding on the Sahamati Central Registry
Description	To enable seamless technical interoperability between AA participants, automated discovery of each other's “addresses” is a must. Sahamati’s Central Registry was created in order to aid the AA ecosystem participants through a unified repository of entity identifiers for interacting with each other in a secure and trustable manner. Currently, all AA ecosystem participants are onboarded on Sahamati’s Central Registry. Hence, each participant who wishes to make themselves discoverable to other participants, and to discover other participants, must be onboarded on Sahamati’s Central Registry. The Central Registry is a list of the public IPs published by each participant, stored securely, in a highly-available environment. It offers an API to other enlisted AA participants (only), for them to pull the public IPs (and other metadata) of participants they have to connect to. In addition to public IPs of each participant, the Central Registry also stores and provides the public key (used for validating digital signatures) and other metadata (e.g. Customer Identifier types and Financial information types supported by FIPs) that are necessary for AAs/FIUs/FIPs to have access to. The Central Registry is hosted by Sahamati and provided to ecosystem participants as a digital common in a secure, highly-available environment.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC002
Target	FIUs, AAs, FIPs

audience	
Purpose	To clarify the need to use the Sahamati Token service
Description	An adjunct to the Central Registry Service is the Sahamati Token service. The open API specifications published by ReBIT mandate that API call authorisation is done on the basis of callers being authenticated via API tokens presented by them. Such API tokens ought to be issued and validated using a standard protocol to ensure authentication and authorisation mechanisms are uniformly applied amongst all ecosystem participants. The AA community has therefore devised the following mechanisms: ● A shared, standardised token issuance service that all participants can use to procure standard, short-lived API tokens ● A common authorisation logic that all participants implement within their systems to verify if API tokens are valid. The Sahamati Token Service, as the name suggests, only issues short-lived API tokens to API callers. It does not validate tokens and as such, is not used by API providers for authorising API calls.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	N/A

2. Technical Interoperability

Code of Conduct No.	CC003
Target audience	FIUs, AAs, FIPs
Purpose	To clarify that FIUs, AAs and FIPs must ensure that their technical implementations are as per ReBIT specifications to ensure that all FIUs and FIPs are compatible i.e. technically interoperable with all AAs and vice versa.
Description	Interactions in the AA ecosystem are designed as bilateral communications between an FIU and an AA or between an FIP and an AA. As per the latest ReBIT specifications, there are no direct API interactions between an FIU and an FIP. Technical interoperability refers to the ability of FIUs and FIPs to interact with every AA as per the standard technical protocol(s) issued by ReBIT.

	Accordingly, FIUs and FIPs must ensure that they implement all technical FIU and FIP standards and protocols respectively, issued by ReBIT in this regard from time to time. Likewise, AAs must also ensure that they implement all technical AA standards and protocols issued by ReBIT in this regard from time to time.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC004
Target audience	FIUs, AAs, FIPs
Purpose	To clarify that if an FIU, AA or FIP is engaging a technology service provider to implement their AA module, the API implementation(s) facilitated by the TSP must be as per the technical specifications issued by ReBIT in this regard, to ensure technical interoperability.
Description	If any FIU, AA or FIP is engaging a technology service provider offering data standards services to integrate such FIU, AA or FIP, as the case may be, in the AA ecosystem, then such TSP must be instructed to ensure that its implementation of the technical specifications for such FIU/ AA/ FIP is strictly as per those prescribed by ReBIT at all times. Such implementation of the ReBIT technical specifications by the technology service provider is imperative to provide technical interoperability for the FIU, AA or FIP, as the case may be. FIUs and FIPs need NOT engage with multiple technology service providers in order to have the technical ability to engage with all AAs. Similarly, AAs also need NOT engage with multiple technology service providers in order to have the technical ability to engage with all FIUs and FIPs. However, AA participants are free to engage with multiple technology service providers for other reasons - such as for the design of redundancy, better service levels, and the like.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

3. Grievance and Dispute Resolution

Code of Conduct No.	CC005
Target audience	FIUs, AAs, FIPs
Purpose	To clarify the definition of a "customer grievance", "grievance" versus a "dispute" amongst Sahamati members and other regulated entities participating in the AA ecosystem
Description	"Customer grievance" refers to a query/ complaint raised by a customer on an FIU, AA or FIP regarding such entities' handling of the consent and/or data through the AA framework. "Grievance" refers to a query/ complaint raised by a Sahamati member or other participant, against another Sahamati or participant pertaining to their operations/ conduct in the AA ecosystem. Such Sahamati member(s) or other regulated entity(ies) participating in the AA ecosystem may operate in any role i.e. as an FIU, AA and/or an FIP. "Dispute" refers to instance(s) when a Grievance remains unresolved beyond the period for resolution prescribed by Sahamati, or is not resolved to the satisfaction of the person raising a grievance.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC006
Target audience	FIUs, AAs, FIPs
Purpose	To clarify who is responsible for grievance redressal in the AA ecosystem.
Description	For Customer grievances: As per the AA Master Directions, Account Aggregators must have a board-approved policy, a dedicated set up and an SLA of no more than a month for disposing of customer grievances.

	FIUs and FIPs may also frame an appropriate customer grievance redressal policy to handle AA-related grievances of their customers, in addition to such customer grievance redressal mechanisms required under applicable legal and regulatory requirements. Such AA-specific mechanisms may involve integrating their systems with the grievance redressal system of an AA, to offer a unified response to the end customer. For grievances/disputes raised by AA participants: Grievances and/ or disputes arising between Sahamati members relating to their participation in the AA ecosystem shall be handled as per the Sahamati Inter Member Dispute Resolution Rules. Non-members of Sahamati may independently ascertain the methodology for grievance and dispute redressal between two or more participants.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC007
Target audience	FIUs, AAs, FIPs
Purpose	To clarify the dispute resolution mechanisms to be made available for customer grievances
Description	If a customer grievance escalates to it becoming a “dispute”, one or both of the following resolution mechanisms are available: ● The aggrieved party may approach the RBI ombudsman (or any other ombudsman under scheme(s) prescribed by the relevant regulator). ● The aggrieved party may avail any other legal recourse available to it.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

4. Technical Implementation

Code of Conduct No.	CC008
Target audience	FIUs, AAs, FIPs
Purpose	To clarify that all participating entities must adhere to the API Specs and FI Schema prescribed by ReBIT
Description	All entities participating in the AA ecosystem must ensure that their technical implementations are aligned with the API specs and FI schema prescribed by ReBIT from time to time. https://api.rebit.org.in/
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

Code of Conduct No.	CC009
Target audience	FIUs, AAs, FIPs
Purpose	To consolidate the Security Standards for all entities participating in the AA ecosystem
Description	All FIUs, AAs and FIPs must ensure that they remain compliant with the Security Standards linked below, along with any relevant requirements prescribed by ReBIT from time to time. https://sahamati.gitbook.io/security-standards
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

5. Data Request Management

Code of Conduct No.	CC010
Target audience	FIUs, AAs, FIPs
Purpose	To clarify that all FIUs, AAs and FIPs must adhere to the guidelines on Session ID and FI Status states
Description	All FIUs, AAs and FIPs must adhere to the guidelines on Session ID and FI Status states. This helps ensure that all participating entities are able to communicate with each other in a consistent and reliable manner. These guidelines are available at https://github.com/Sahamati/certification-framework/blob/main/guidelines/session-id-and-fi-status-states.md
Treatment	Mandatory
Published on	August 31, 2022
Modified on	N/A

6. API Implementation Best Practices

Code of Conduct No.	CC011
Target audience	FIUs, AAs, FIPs
Purpose	To clarify implementation requirements regarding technical aspects of the API specifications
Description	All FIUs, AAs and FIPs must adhere to the General Guidelines for implementation contained in the below guidelines: https://github.com/Sahamati/certification-framework/blob/main/guidelines/general-guidelines.md
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

7. Certification Framework

Code of Conduct No.	CC012
Target audience	FIUs, AAs, FIPs
Purpose	To clarify the need for "Certification"
Description	"Certification" is essentially a technical guarantee of adherence to the open API specifications published by ReBIT. The Certification framework comprises three community-defined elements: ● An open (i.e. non-proprietary) suite of test cases, complementing the open API specifications - designed by the community ● A set of third-party certifiers, empaneled by Sahamati ● Sahamati Certification Guidelines – A set of rules governing the process of certification The benefit of being certified is that it provides a guarantee of "good behaviour" (technically) to other members of the ecosystem, thus generating trust amongst AA participants and customers, reducing the count and cost of downstream errors and grievances. The open test cases of the certification framework form part of a stack of Digital Commons designed and driven by the community. They are not part of RBI Master Directions or ReBIT Technical Specifications. As per the Sahamati Membership Terms, all Sahamati members must ensure that they are duly certified at all times as per the Sahamati Certification Guidelines.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC013
Target audience	FIUs, AAs, FIPs
Purpose	To clarify the frequency and need for re-certification

Description	Once certified for a particular version of the specifications, an entity need not be recertified so long as the entity is on the same version. Re-certification would be required in all circumstances defined in the Sahamati Certification Guidelines. Periodic self-tests as per the Sahamati Certification Guidelines are recommended.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC014
Target audience	FIUs, AAs, FIPs
Purpose	To clarify that a holding company cannot be certified on behalf of its subsidiary FIUs
Description	The intent of the Sahamati Certification Guidelines is to ensure AA ecosystem participants can demonstrate a technical guarantee of their implementations adhering to the ReBIT technical specifications. A holding company that is not an FIU, AA or an FIP cannot provide this guarantee on behalf of other companies, even if there is a shareholding relationship amongst them, and therefore, cannot be treated as a certified entity in the AA ecosystem.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

CHAPTER II

Codes of Conduct for FIUs

1. Account Discovery

Code of Conduct No.	CC015
Target audience	FIUs, AAs
Purpose	To clarify that FIU(s) can pass the name(s) of FIP(s) to an AA for the purpose of account discovery if such FIP(s) are *specified* by the customer on the FIU interface
Description	When a customer specifies the names of FIP(s) to an FIU on the FIU interface for the purpose of account discovery, such FIP(s) name(s) may be passed by the FIU to the AA for discovering the customer's account(s) through an integration between the FIU front-end and the AA client. The AA can execute account discovery calls on the specified FIP(s). This is to support customer journeys that originate on the FIU front-end and involve embedded AA interactions.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

2. Consent Request Management

Code of Conduct No.	CC016
Target audience	FIUs
Purpose	To clarify that an FIU cannot request for an irrevocable consent
Description	A consent artefact can never be "irrevocable". Consequently, there is no scope for a consent request to be placed such that the consent is irrevocable. All consent requests placed in the AA ecosystem must be revocable. This is aligned with the underlying principles of the AA Master Directions as well as the Digital Personal Data Protection Act, 2023.

Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC017
Target audience	FIUs
Purpose	To clarify: a. the maximum period of "Data Storage" for an FIU; and b. the difference between "Data Life" and "Data Storage"
Description	The consent request placed by an FIU includes a parameter called 'Data Life'. This represents the period that the FIU may "process" the raw data, once received through the AA pursuant to the customer's consent. As defined in the open API specification of the electronic consent artefact, 'Data Life' refers to the time window declared by an FIU for "processing" or "using" the data shared by a customer, for the purpose declared. E.g. a lender may declare a Data Life of 24 hours, to process the data shared by a borrower for underwriting a loan application. In such case, the lender should process the data within 24 hours of receiving the data, for the stated purpose. FIUs are expected to "delete" the raw data, after the Data Life time-window expires. Here, the term "delete" is to be interpreted as a "soft delete", since FIUs may have to retain the data as per applicable legal and regulatory requirements regarding archival of such data collected by the FIU. In other words, the FIU should not 'use' the data beyond the Data Life, but may "store" / "archive" the data as per applicable legal and regulatory requirements. Data Life is different from 'Data storage'. Data Storage defines the maximum period for which the FIU stores/archives the data as per its policy, for purposes such as aiding in any customer/other queries, grievances or disputes that may arise, or as per legal requirements, beyond the period for which the raw data is processed i.e. Data Life. Thus, an FIU is expected to continue adhering to existing legal and regulatory norms with respect to "storage of data", where it is understood that such stored data is not meant to be "processed" or "used" in any manner, other than dictated by existing legal and/or regulatory norms. These codes of conduct do not, in any manner, influence data storage laws or

	regulations applicable to any particular FIU.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC018
Target audience	FIUs
Purpose	To clarify what the term “FI Data Range” represents
Description	FI Data Range represents the entire range of time for which data may be fetched. In case of consents with validity extended into the future, FI Data Range shall also include such period. E.g. If on August 1st 2022, the consent is being sought, for data to be fetched for 6 months prior and till 12 months into the future, the FI Data Range will be “From Feb 1st 2022” and “To July 31st 2023”.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC019
Target audience	FIUs, AAs
Purpose	To clarify norms for how consent request attributes should be presented on AA Client interfaces (on FIU or AA properties) to customers
Description	RBI Master Directions direct AAs as follows: *“6.5 At the time of obtaining consent, the Account Aggregator shall inform the customer of all necessary attributes to be contained in the consent artefact as per paragraph 6.3 above and the right of the customer to file complaints with relevant authorities in case of non-redressal of grievances.”*

	The "inform customer of all necessary attributes" is to be implemented on AA client (web app, mobile app, e.g.) screens in a manner which neither overwhelms the customer nor makes it incomprehensible. ReBIT's API specification gives practical shape to this requirement by defining a detailed consent artefact containing over 15 attributes. These attributes collectively ensure that all necessary information – such as data type, frequency, purpose, and duration, is part of the customer's consent record. Thus, the RBI's legal requirement (Clause 6.5) and ReBIT's technical specification must be read together – the regulation establishes the obligation to inform, while the API standard defines what constitutes a complete and informed consent. All FIUs and AAs must ensure that the consent attributes displayed to the customers are as per the relevant Fair Use Template(s). The community has also devised a set of recommended guiding principles which have been published in the form of a checklist for participating entities: Customer Experience Checklist – available here customer-experience-guidelines/consent-guidelines.md at main · Sahamati/customer-experience-guidelines · GitHub
Treatment	Mandatory
Published on	August 31, 2022
Modified on	February 23, 2024; June 11, 2025

3. Data Request Management

Code of Conduct No.	CC020
Target audience	FIUs
Purpose	To clarify that FIUs should not repeat presenting a specific data request to depositories or RTAs, within a given calendar day, if the data against such a specific data request has already been received successfully.
Description	As per the ReBIT data schema for the FI Types made available by depositories and RTAs, such FIPs can only provide data (profile, summary, transactions) as of the previous day's closing. The data provided in each request will remain identical until the next day's closing, irrespective of the number of times a specific data request is submitted to these FIPs in the interim.

	For instance, where the data **request** for the same consent ID and the same FI Data Range is sent multiple times in a calendar day, all data **fetches** made during the calendar day (for the same consent ID but without the optional attribute of the link reference number), will yield the same information. In light of this, **only one data request** should be made **in a calendar day** for a given Consent Artefact and a given FI Data Range, provided data is successfully received against that request.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

4. Consent Lifecycle Management

Code of Conduct No.	CC021
Target audience	FIUs, FIPs
Purpose	To clarify the mechanism for a customer to *initiate* the process of revoking a consent via an FIU or an FIP channel, instead of directly on the AA interface
Description	A customer should be able to initiate his/her intent to revoke a consent on an FIU or an FIP channel, which may be designed as per the FIU's or FIP's preference. The intent to revoke, once demonstrated to the FIU/ FIP by the customer, should result in the customer a. either being re-directed digitally to the AA that the customer has used previously, for the customer to complete the process of revocation, or b. being provided information as to how the customer can independently invoke the AA's interface and complete the process of revocation. It is strongly recommended that FIUs and FIPs implement point (a) above, to enable ease for customers. In this context, ReBIT has clarified in its FAQs as follows: *"FIP or FIU can use the POST /Consent/Notification API hosted by AA to raise a consent status update request to revoke consent. AA can perform the actual consent status update as per the request received after customer confirmation and notify FIP/FIU."*

Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

5. FIU roles and responsibilities

Code of Conduct No.	CC022
Target audience	FIUs
Purpose	To clarify that an FIU will need to obtain a unique entry in the central registry for each FIU end-point.
Description	An FIU may have multiple deployments of its FIU gateway, either to serve different departments within its FIU or as a technical redundancy measure. Each such gateway **must** have its own public IP, public keys. In the current version of the central registry and token service, each such gateway will have its own entry, with its own unique FIU ID.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC023
Target audience	FIUs
Purpose	To clarify that a holding company that is not a registered and regulated entity itself cannot be considered an FIU
Description	The AA Master Directions explicitly define FIUs as only such entities that are directly "registered with and regulated by" a financial sector regulator can be considered an FIU. Any other entity, including parent/holding companies of such an entity, are not eligible to be an FIU.

Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC024
Target audience	FIUs
Purpose	To clarify the meaning of ‘reciprocity obligation’ and that it is obligatory for a financial institution acting as an FIU to also be an FIP.
Description	Each financial institution is free to determine if it wishes to participate in the AA ecosystem or not. The term “Reciprocity” refers to an implicit obligation of a financial institution to play two roles, in the AA ecosystem - that of an FIU and that of an FIP, excluding certain FIPs which are not in a position to act as an FIP. In other words, every financial institution wishing to join the AA ecosystem as an FIU (a “user” of information) must also agree to be an FIP (a “provider” of information), provided they hold financial information types that can be shared through the AA framework as per extant ReBIT technical specifications. Thus, if a financial institution chooses to join the AA ecosystem as an FIU, a community-designed implicit obligation of “Reciprocity” applies to such an institution. This has been further clarified as a requirement under clause 7.7 of the AA Master Directions as under: *“7.7 Joining the Account Aggregator Ecosystem as Financial Information User* *With a view to ensure efficient and optimum utilisation of the Account Aggregator ecosystem, regulated entities of the Reserve Bank joining the Account Aggregator ecosystem as Financial Information User shall necessarily join as Financial Information Provider also, if they hold the specified financial information and fall under the definition of Financial Information Provider.”*
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

6. Fair Use

Code of Conduct No.	CC025
Target audience	FIUs, AAs
Purpose	To clarify the mapping between FIU use cases and the purpose codes to be used, for the known use case categories
Description	ReBIT defines and maintains the list of Purpose Code under ReBIT specifications for AA ecosystem: https://api.rebit.org.in/purpose As per the latest publication, there are five purpose codes under three categories. The categories and purpose descriptions are broad and can accommodate several use cases within each purpose code. Under the fair use framework, the User Councils anchored by Sahamati, comprising several participating FIUs, have collaborated to agree on the most appropriate purpose code for each known use case, to promote predictability and consistency in implementation across the ecosystem. A mapping between ReBIT defined purpose codes and the known use cases as per the Fair Use Template Library can be found at https://sahamati.org.in/aa-fair-use-template-library/
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	December 02, 2022; February 23, 2024; June 11, 2025

Code of Conduct No.	CC026
Target audience	FIUs
Purpose	To clarify that multiple financial services or processes cannot be tied to one purpose and one consent artefact
Description	The intent behind the concept of “purpose-limitation” is to ensure there is a one-to-one mapping between the customer’s understanding of the purpose for which the FIU is seeking the financial information and legal basis for the FIU to process such information. The purpose can be for a financial service and/or a process to avail a financial service.

	Financial services refer to loans, insurance, financial advisory etc., while processes include the process of loan underwriting, loan monitoring, assessing risk for advisory, etc. For instance, consider a financial service such as a loan. It involves two separate processes: a) one for assessing the customer's eligibility for the loan, and b) another for monitoring the repayment risk of the loan. Even though it's the same financial service (the loan), there are two distinct purposes, and two data sets are required for the two different purposes – So, two different consents are needed. Accordingly, an FIU should not bundle two purposes into one consent request. If a financial service involves the opening of multiple accounts as part of a single transaction (e.g., often, opening of a loan account also involves opening of a deposit account simultaneously), the "purpose" is deemed to be the same. In such a situation, the same should be conveyed to the customer unambiguously so the customer is aware that the data received by the FIU will be used for the purpose specified and for activities that are intrinsically linked and conjoined. However, the converse – where data is taken for one specific financial service or process but used, additionally or in its place, for another financial service or process, that the customer is not explicitly seeking – will not be in compliance with applicable legal and regulatory frameworks.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	December 02, 2022; June 11, 2025

Code of Conduct No.	CC027
Target audience	FIUs
Purpose	To clarify that use of Purpose Code 102 should be strictly as per the regulatory charter(s)/ licence(s) of the relevant FIU
Description	FIUs relying on Purpose Code 102 i.e. "*Customer spending patterns, budget or other reportings*' under the category '*Personal Finance*' must ensure that their use case implementation(s) in the AA ecosystem are clearly within the scope of their regulatory charter(s). As per the deliberations in the User Councils, it is clarified that the Purpose Code itself is primarily intended to generate insights based on your overall finances and provide incidental recommendations (if any) derived from an advisory element in their charter. The User Councils also clarified that the Purpose Code in itself does not expand the scope of any

	regulatory charter(s)/ licence(s). In other words, recommendations for personal finance management, including nudges for products and services, if any,, must be permitted under an FIU's relevant regulatory charter(s). For instance, in order to provide nudges/ recommendations for insurance products or services, the FIU should possess a valid licence from IRDAI permitting the concerned FIU to engage in such activities. Similarly, to provide recommendations on investment advice, the FIU should possess a valid licence from SEBI that allows the FIU to offer investment advice.
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

Code of Conduct No.	CC028
Target audience	FIUs
Purpose	To clarify that if an FIU makes a recommendation for a product or service under Purpose Code 102 based on their regulatory charter/ licence, a separate consent must be sought to process the customer's application of such recommended product or service
Description	If an FIU recommends a product or service to a customer under Purpose Code 102, the FIU should not use the same consent for servicing the customer for such product/ service. In other words, a separate consent must be sought from the customer to fetch data for processing the application for such a product or service. It is to be noted that the purpose of data processing under Purpose Code 102 is to recommend products and/ or services to the customer, whereas processing the customer's application for such a product and/or service would amount to a separate and distinct purpose. This also upholds the spirit of purpose limitation principles adopted in the Digital Personal Data Protection Act, 2023. For instance, if an FIU recommends an insurance policy to the customer under Purpose Code 102, and the customer proceeds to make an application with such FIU for the policy, the FIU must seek a separate consent for underwriting the insurance policy as per the relevant fair use template from the Fair Use Template Library published by Sahamati.
Treatment	Mandatory

Published on	June 11, 2025
Modified on	N/A

Code of Conduct No.	CC029
Target audience	FIUs
Purpose	To clarify consent validity under the fair use templates CT003 (Loan Monitoring) and CT035 (Account Monitoring for Collections) for short-term loans
Description	This is to clarify that for short-term loans, i.e., loans for less than one year, the validity of consent **must not be more than 3 months beyond the tenure** of the loan. The Lending User Council under Sahamati's Fair Use Committee has recommended this to enable lenders to continue monitoring a borrower's account and optimise their collection strategies in case a borrower delays repayment. The rationale being that lenders offering short-term loans, especially unsecured, are at higher risk of default and need flexible collection strategies because of the limited ageing of the particular loan account. Eg.: if the loan tenure is two months, the consent validity can be up to five months.
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

Code of Conduct No.	CC030
Target audience	FIUs
Purpose	To clarify that FIUs may only fetch incremental data in cases of recurring consents
Description	When fetching data on the basis of a recurring consent, FIUs are expected to seek **only incremental data** from the last successful data fetch. This means that data fetch requests should be limited to FI data range from the last successful data fetch. A buffer period of 7 days may be maintained to ensure accuracy and to account for any potential delays or discrepancies in data. This buffer period is calculated from the last successful data fetch (T minus the last successful data fetch).

	The 7-day buffer period has been established to address delays and discrepancies that might occur, especially in cases involving forex transactions. This buffer allows for correction of any potential issues and helps ensure that all relevant data is captured accurately.
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

Code of Conduct No.	CC031
Target audience	FIUs
Purpose	To clarify that the FI Date Range displayed to the customer should be classified for non-SEBI and SEBI FI Type in the consent notice
Description	The FI Date Range for SEBI-regulated FI types may be longer than that for non-SEBI FI types. This distinction is based on the decisions documented in the Fair Use Template Library available at: https://sahamati.org.in/aa-fair-use-template-library/ When a consent request includes both SEBI and non-SEBI FI types, FIUs must clearly indicate the respective date ranges for each in the consent notice. This helps ensure transparency and avoids confusion for customers by making it clear to the customer that their bank statements are not being fetched for the same extended period as their investment data. This clarity is essential for maintaining informed consent and customer trust.
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

Code of Conduct No.	CC032
Target	FIUs

audience	
Purpose	To clarify that an overriding consent on-top-of a consent for data obtained through the AA framework is not permitted
Description	This is to clarify that FIUs must not seek an overriding/ wrapper consent on top of a consent for data to be fetched through the AA framework. It is crucial to limit the scope of use of the data to the original purpose for which the consent/ data is sought. Thus, if an FIU is seeking consent for a specified purpose through the AA framework, it should not seek additional consents in respect of such data to modify/ expand the original purpose of seeking the data. For instance, if an FIU is seeking a recurring consent for fetching a customer's data for monitoring a loan, it should not use such data for any additional purpose such as cross-sell/ up-sell through an additional consent sought from the customer elsewhere in the user journey. This is aligned with the purpose and usage limitation principles under the DPDP Act, as well as Clause 7.6.2 of the AA Master Directions read with the ReBIT technical specifications, which envisage: a. seeking separate consents from a customer/ data fetches, for separate purposes; and b. Not using data obtained for a specific purpose for a different purpose
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

Code of Conduct No.	CC033
Target audience	FIUs
Purpose	To prescribe the technical guardrails for FIUs implementing Fair Use Template CT 003 (Loan Monitoring) and/ or CT 035 (Account Monitoring for Collections)
Description	FIUs engaging in loan monitoring and collection related use cases as per Fair Use Templates CT 003 and CT 035 must strictly take the following measures to uphold the principles of collection, purpose and usage limitations. FIUs must: **A. Provide appropriate disclosure(s):**

	FIUs must provide an appropriate disclosure to the customer (as a part of the purpose text) that: 1. Monitoring consent will be activated only if the loan is disbursed; and 2. Collection consent will be activated only if the loan is under default. **B. Minimise data collection:** FIU must ensure, technically, that: 1. Data against monitoring consent is pulled only for active loans; and 2. Data against collection consent is pulled only if the payment under the loan (EMI) is overdue for more than a day. **C. Enable consent revocation when purpose fulfilled/ no longer necessary:** FIUs must ensure that in instances of a rejected/ prepaid loan i.e. when the underlying purpose is fulfilled and further data is no longer necessary for the stated purpose, the customer is provided, as a part of their user journey, an option to revoke the existing monitoring consent and collection consents. As a best practice, to enable the customer to revoke their live consent, FIUs should present a redirection link to the AA page/app or through any other communication channel (in case of non-STP journeys). Further, even if a customer in such cases does not revoke the consent(s), the FIUs must implement appropriate internal technical mechanisms to ensure that no customer data is fetched if the purpose is fulfilled or no longer necessary.
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

Code of Conduct No.	CC034
Target audience	FIUs
Purpose	To provide for the technical guardrails for FIUs implementing Fair Use Template CT 040 (Bank Account Verification)
Description	To ensure that FIUs avoid fetching customer data from multiple accounts for the purpose of customer profile/ bank account verification, it was agreed in the Cross Sector User Council facilitated by Sahamati that only 1 (one) financial account of the customer may be fetched, in order to maintain a single source of

	truth. Such accounts may be from FI Types amongst those permitted under CT040 i.e. DEPOSITS, GSTB1_3B, LIFE_INSURANCE, GENERAL_INSURANCE.
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

7. AA Client Integration

Code of Conduct No.	CC035
Target audience	FIUs, AAs
Purpose	To clarify that the AA Client must be owned by AAs, while the interface of such AA Clients can be co-development by AAs with specific FIUs.
Description	An AA Client must necessarily be owned by an AA. As per ReBIT guidelines, an "AA Client" possesses the following characteristics: ● An application that enables customers to interact with the AA for the purposes of registration, account discovery and linking and consent management - thus implying that the "interface" (e.g. a screen) used by the customer during the interaction is considered part of the AA Client; ● Available as either a web application or a mobile application or a library that can be embedded in other web or mobile applications (subject to constraints imposed by security concerns); and ● Owned by an AA. The term "library" is interchangeable with the term "SDK". Further, as mentioned in the first characteristic, the "library" (or "SDK") includes the customer-facing interface (such as a "Screen"). *A "set of APIs" or a "headless library" (i.e. without screens) does not qualify to be called an AA Client*. Such sets of APIs are internal engineering assets of an AA. However, the interfaces (e.g. screens) that are part of the AA Client design may be customised or co-designed by FIUs, in partnership with AAs, to suit their user interface and user experience requirements.

	The co-development scope may include any or all of the following: ● User interface redesign ● User experience (i.e. workflow or sequence of steps that a user experiences) redesign ● Development assistance, supporting the redesign efforts As long as the interaction is bound by common guidelines derived from Master Directions and/or relevant ReBIT technical specifications, FIUs and AAs are free to redesign AA Client interfaces as per their requirements, in compliance with applicable legal and regulatory requirements. Such community-driven guidelines and principles are recommended here: https://github.com/Sahamati/customer-experience-guidelines Further, it is clarified that any redesigned interface screens are also “owned” by the AA, with respect to all aspects of development and devops. As part of a joint design and development effort with respect to the interface screens, AAs may provide access to internal APIs as they deem fit, while retaining complete control over all aspects of development, testing and distribution. FIUs and AAs are, however, free to enter into any bilateral legal agreements to restrict usage of such co-designed interfaces to named parties mutually agreed by them.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC036
Target audience	FIUs, AAs
Purpose	To clarify what metadata, if any, can be communicated between an AA Client and the FIU app
Description	An AA Client may only share with an FIU the parameters specified under the AA Redirection Guidelines. The technical guidelines for *Redirection* and *Mobile library invocation/ app-to-app integration* under the AA Redirection Guidelines provide clarity on what parameters can be passed back-and-forth between the AA Client and the FIU app.

	In addition to parameters that help an AA authenticate the app user (e.g. mobile number) and the FIU determines user experience post-AA-interaction (e.g. whether the user approved a consent request or not), it may be useful for an FIU to determine the termination stage in a user's AA journey. This is useful for the FIU to provide appropriate support for repeat tries / grievance redressal to the customer. In addition to such information pertinent to an individual customer's AA journey, it would also be useful for the FIU to get anonymized, aggregated metadata about its customers' AA journey. Such metadata may include all information necessary for the FIU and the AA to jointly construct a "drop-off funnel" and use the same to improve user experience. The parameters that constitute such "metadata" are as defined here: https://sahamati.gitbook.io/aa-redirection-guidelines/v/1.2.1/specification/response-specification
Treatment	Mandatory
Published on	August 31, 2022
Modified on	February 23, 2024; June 11, 2025

Code of Conduct No.	CC037
Target audience	FIUs, AAs
Purpose	To clarify branding guidelines for co-designed AA Client screens
Description	All AA Client screens that are co-designed with FIUs ought to include "Powered by <AA Name>" along with an appropriate trust marker such as "<RBI registered entity>", in a clearly visible area of the screen. The AA Logo may be optionally added, next to the AA Name.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of	CC038

Conduct No.	
Target audience	FIUs, AAs
Purpose	To clarify that the FIU name and logo should be displayed on AA Client screens in a *redirection* type of integration
Description	AA Client screens should show the FIU name and/or logo, from-and-to which the customer will be redirected. This is to enable contextual continuity to users while switching between the FIU and AA interfaces.
Treatment	Recommended
Published on	August 31, 2022
Modified on	N/A

Code of Conduct No.	CC039
Target audience	FIUs, AAs
Purpose	To clarify that all FIUs and AAs must strictly adhere to the AA Redirection Guidelines
Description	All FIUs and AAs must strictly adhere to the AA Redirection Guidelines, which are available at the below link: https://sahamati.gitbook.io/aa-redirection-guidelines
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

8. Customer Experience

Code of Conduct No.	CC040
Target audience	FIUs, AAs

Purpose	To clarify the recommended standards and design principles for customer experience design and user journeys within AA framework based on community-driven initiatives
Description	All FIUs and AAs should ensure that their customer experience design and user journeys within AA framework are aligned with the minimum standards and design principles outlined in the Sahamati-IDEO Design Report. This report lays out clear key design principles for: 1. The AA flow - Includes educating customers about Account Aggregators before AA Redirection, AA registration and login, as well as discovery and linking of financial accounts with AA account. 2. Informed Consent - Includes Consent Notice screens, Accept, and Reject flows, as well as Error and Success notification screens 3. Consent Revocation - Includes Consent Review/ Management screens, and Revocation screens The Sahamati-IDEO Design Report is available at the link below: https://sahamati.org.in/wp-content/uploads/2023/05/IDEO-LMM-Sahamati-Collab-on-AA-Flow-v1-compressed.pdf It should be noted that the principles underlying the above report should be adhered to in their spirit. All Sahamati Members and other participants should suitably adopt them in their user journeys. Entities should refer to the design principles underpinning the report which are consolidated at the below links: https://github.com/Sahamati/customer-experience-guidelines/blob/main/consent-guidelines.md Reference figma (screens) from the IDEO report is available here.
Treatment	Recommended
Published on	June 11, 2025
Modified on	N/A

CHAPTER III

Codes of Conduct for AAs

1. Customer Registration and de-registration

Code of Conduct No.	CC041
Relevant implementor entity	AAs
Purpose	To clarify AAs' accountability towards customer authentication while enabling a customer to register with it, i.e. get a VUA issued.
Description	Every AA must independently authenticate its customer, prior to issuing a VUA (Virtual User Address) to the customer. This is further to the requirement under clause 5(d) of the AA Master Directions.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC042
Target audience	AAs
Purpose	To clarify that a customer must be allowed to de-register his/her AA profile
Description	Every AA must allow a customer to de-register his/her AA profile. The design of the de-register mechanism is left to each AA. Once de-registered, all active consents attached to that AA profile automatically get revoked and all accounts previously linked become de-linked.
Treatment	Mandatory
Published on	August 31, 2022

Modified on	N/A

2. User Identification and Authentication

Code of Conduct No.	CC043
Target audience	AAs
Purpose	To clarify the Customer Identifiers that an AA must support, for authentication during initial registration and subsequent access
Description	To authenticate a Customer during customer registration, an AA *must* support taking the: ● Mobile number as an identifier To authenticate a customer during subsequent access (i.e. login), an AA *must* support taking either of the two below: ● Mobile number as an identifier ● VUA as an identifier An AA *may* also support identification and authentication using the below identifiers if a specific use case warrants the same: ● Email address ● Aadhar number
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

3. Account Discovery

Code of Conduct No.	CC015
Target audience	AAs, FIUs
Purpose	To clarify that FIU(s) can pass the name(s) of FIP(s) to an AA for the purpose of account discovery if such FIP(s) are *specified* by the customer on the FIU interface
Description	When a customer specifies the names of FIP(s) to an FIU on the FIU interface for the purpose of account discovery, such FIP(s) name(s) may be passed by the FIU to the AA for discovering the customer's account(s) through an integration

	between the FIU front-end and the AA client. The AA can execute account discovery calls on the specified FIP(s). This is to support customer journeys that originate on the FIU front-end and involve embedded AA interactions.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC044
Target audience	AAs
Purpose	To clarify if account discovery can be done using an identifier that is different from what the user provided during registration with the AA
Description	To enable a user to discover their accounts linked with different mobile numbers across FIPs, a user may provide different identifier(s) (e.g. mobile number or email ID) for enabling discovery of their accounts from one or more FIPs, than what was provided during registration with the AA. ● The different identifier(s) provided must include at least one strong identifier (i.e. mobile number or email ID) ● The AA must authenticate the new identifier as well, before sending the discovery request to the FIP As per ReBIT, (as given here) strong identifiers include: 1. Mobile number; 2. Email address; and 3. Aadhaar number. Weak and ancillary identifiers include: 1. PAN; 2. DOB; and 3. Other suitable identifiers.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC045
Target audience	AAs, FIPs
Purpose	To clarify what are considered "Strong Identifiers" for Discovery and whether additional identifying attributes can be added to these
Description	As per ReBIT, (as given here) strong identifiers are one of the following: ● Mobile Number ● Email ID ● Aadhaar Number Additional identifiers, such as Date of Birth, PAN - can be added, as required by each FIP, as per ReBIT Circular No. ReBIT/AA/2024-25/01 dated January 10, 2024. All additional identifiers must be clubbed with the Strong Identifier value using an "AND" condition. The type of identifiers supported for discovery at an FIP's end are stored against each FIP's entry in the Central Registry.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	February 23, 2024; June 11, 2025

Code of Conduct No.	CC046
Target audience	AAs
Purpose	To clarify that an AA cannot share information about "discovered accounts" with FIUs
Description	The information provided by FIPs in response to a discovery request is meant only for the AA. Such information cannot be shared by the AA with an FIU. FIUs can only get information for accounts that are included by the customer in the consent artefact while approving the FIU's consent request(s).

Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

4. Technical Interoperability

Code of Conduct No.	CC047
Target audience	AAs
Purpose	To clarify that technical interoperability does not imply AAs sharing information amongst each other
Description	Technical interoperability does not imply AAs sharing information with each other. Each AA operates as an independent entity, performing the business it is licensed to. Customers have a choice of which AAs they would like to use. Customers are free to choose one or more such AAs. Consents (and associated data flows) managed via one AA are not shared by that AA with other AAs.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	N/A

5. Consent Request Management

Code of Conduct No.	CC019
Target audience	FIUs, AAs
Purpose	To clarify norms for how consent request attributes should be presented on AA Client interfaces (on FIU or AA properties) to customers
Description	RBI Master Directions direct AAs as follows:

	"6.5 At the time of obtaining consent, the Account Aggregator shall inform the customer of all necessary attributes to be contained in the consent artefact as per paragraph 6.3 above and the right of the customer to file complaints with relevant authorities in case of non-redressal of grievances." The "inform customer of all necessary attributes" is to be implemented on AA client (web app, mobile app, e.g.) screens in a manner which neither overwhelms the customer nor makes it incomprehensible. ReBIT's API specification gives practical shape to this requirement by defining a detailed consent artefact containing over 15 attributes. These attributes collectively ensure that all necessary information – such as data type, frequency, purpose, and duration, is part of the customer's consent record. Thus, the RBI's legal requirement (Clause 6.5) and ReBIT's technical specification must be read together – the regulation establishes the obligation to inform, while the API standard defines what constitutes a complete and informed consent. All FIUs and AAs must ensure that the consent attributes displayed to the customers are as per the relevant Fair Use Template(s). The community has also devised a set of recommended guiding principles which have been published in the form of a checklist for participating entities: Customer Experience Checklist – available here customer-experience-guidelines/consent-guidelines.md at main · Sahamati/customer-experience-guidelines · GitHub
Treatment	Mandatory
Published on	August 31, 2022
Modified on	February 23, 2024

6. Customer as a data recipient

Code of Conduct No.	CC048
Target audience	AAs
Purpose	To clarify that a customer can be a recipient of her own data via an AA
Description	As per the RBI Master Directions, an AA's charter is to enable (amongst other things) presentation of a customer's data to herself.

	Given that an AA is data-blind, this implies that an AA can deliver encrypted data to the customer's device. Further, to enable presentation of data received by the device, an AA Client (front-end application) that is resident on the device of the customer (such as a mobile app) may offer the feature of on-device decryption and presentation of the customer's data to her. Under no circumstances is the decrypted data allowed to be processed or stored on the servers of the AA, since that is in contravention to the principle of the AA being data-blind.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	February 23, 2024; June 11, 2025

7. Fair Use

Code of Conduct No.	CC025
Target audience	FIUs, AAs
Purpose	To clarify the mapping between FIU use cases and the purpose codes to be used, for the known use case categories
Description	ReBIT defines and maintains the list of Purpose Code under ReBIT specifications for AA ecosystem: https://api.rebit.org.in/purpose As per the latest publication, there are five purpose codes under three categories. The categories and purpose descriptions are broad and can accommodate several use cases within each purpose code. Under the fair use framework, the User Councils anchored by Sahamati, comprising several participating FIUs, have collaborated to agree on the most appropriate purpose code for each known use case, to promote predictability and consistency in implementation across the ecosystem. A mapping between ReBIT defined purpose codes and the known use cases as per the Fair Use Template Library can be found at https://sahamati.org.in/aa-fair-use-template-library/
Treatment	Clarificatory
Published on	August 31, 2022

Modified on	December 02, 2022; February 23, 2024; June 11, 2025

Code of Conduct No.	CC049
Target audience	AAs
Purpose	To clarify the technical guardrails to be adopted by AAs to enable self-use by customers based on CT 019 (Self Use consent on AA apps)
Description	For AAs enabling customers to engage in self-use scenarios on AA apps (mobile or web) i.e. where the customer is the direct recipient of their financial data, AAs must strictly ensure that the following guardrails are implemented by them: **A. Security Preconditions for Enabling Self-Use Functionality** Self-use functionality enabled through CT019 must only be activated in AA apps (mobile or web) after implementation of robust security controls, including: ● Mandatory two-factor authentication (2FA); and ● Device-SIM binding to ensure account integrity These controls are essential to prevent unauthorised access, especially in cases of device theft or SIM reallocation. The self-use feature must not be activated unless these minimum standards are met across the AA's app ecosystem. **B. Implement Download Restrictions and User-Controlled Sharing** While CT019 allows users to view their financial data, download functionality (if provided by the AA app) must adhere to the following safeguards: ● All downloaded files must be password-protected, with the password set or confirmed by the customer. Subject to the applicable legal and regulatory standards, while an AA may allow manual file sharing by the customer, auto-fetch and/ or auto-sharing features are strictly disallowed on AA apps.
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

8. AA Client Integration

Code of Conduct No.	CC035
Target audience	FIUs, AAs
Purpose	To clarify that AA Client must be owned by AAs. The interface of such AA Clients can be co-development by AAs with specific FIUs.
Description	An AA Client must necessarily be owned by an AA. As per ReBIT guidelines, an "AA Client" as possessing the following characteristics: ● An application that enables customers to interact with the AA for the purposes of registration, account discovery and linking and consent management - thus implying that the "interface" (e.g. a screen) used by the customer during the interaction is considered part of the AA Client; ● Available as either a web application or a mobile application or a library that can be embedded in other web or mobile applications (subject to constraints imposed by security concerns); and ● Owned by an AA. The term "library" is interchangeable with the term "SDK". Further, as mentioned in the first characteristic, the "library" (or "SDK") includes the customer-facing interface (such as a "Screen"). *A "set of APIs" or a "headless library" (i.e. without screens) does not qualify to be called an AA Client*. These sets of APIs are internal engineering assets of an AA. However, the interfaces (e.g. screens) that are part of the AA Client design may be customised or co-designed by FIUs, in partnership with AAs, to suit their user interface and user experience requirements. The co-development scope may include any or all of the following: ● User interface redesign ● User experience (i.e. workflow or sequence of steps that a user experiences) redesign ● Development assistance, supporting the redesign efforts As long as the interaction is bound by common guidelines derived from Master Directions and/or relevant ReBIT technical specifications, FIUs and AAs are free to redesign AA Client interfaces as per their requirements, in compliance with applicable legal and regulatory requirements.

	Such community-driven guidelines and principles are recommended here: https://github.com/Sahamati/customer-experience-guidelines Further, it is clarified that any redesigned interface screens are also "owned" by the AA, with respect to all aspects of development and devops. As part of a joint design and development effort with respect to the interface screens, AAs may provide access to internal APIs as they deem fit, while retaining complete control over all aspects of development, testing and distribution. FIUs and AAs are, however, free to enter into any bilateral legal agreements to restrict usage of such co-designed interfaces to named parties mutually agreed by them.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC050
Target audience	AAs
Purpose	To clarify that an embedded Web Library is not an acceptable form of an AA Client
Description	Embedded Web libraries (e.g. those built using Javascript) pose a serious data privacy risk. Applications that embed such web libraries, in their web applications, are likely to gain control over data that flows to-and-fro between the library and the backend service. Such risks can be mitigated technically for mobile libraries (e.g. built using Android, iOS) embedded within host mobile applications. They cannot be mitigated for web libraries. Therefore, no AA should offer an embedded web library to FIUs as an AA Client.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC051
Target audience	AAs
Purpose	To clarify what “ownership” of an AA Client implies
Description	An AA Client is necessarily “owned” by an AA. This implies the following: For AA Client of type = web application: ● Ownership of the application code and its underlying infrastructure (including the environment the application is hosted on) has to reside with the AA For AA Client of type = mobile application OR mobile library: ● Ownership of the application code, distribution of the applications, ownership of the distributed app packages has to reside with the AA The accountability of all aspects pertaining to the AA Client rests solely with the AA.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	N/A

Code of Conduct No.	CC036
Target audience	FIUs, AAs
Purpose	To clarify what metadata, if any, can be communicated between an AA Client and the FIU app
Description	An AA Client may only share with an FIU the parameters specified under the AA Redirection Guidelines. The technical guidelines for *Redirection* and *Mobile library invocation/ app-to-app integration* under the AA Redirection Guidelines provide clarity on what parameters can be passed back-and-forth between the AA Client and the FIU app.

	In addition to parameters that help an AA authenticate the app user (e.g. mobile number) and the FIU determines user experience post-AA-interaction (e.g. whether the user approved a consent request or not), it may be useful for an FIU to determine the termination stage in a user's AA journey. This is useful for the FIU to provide appropriate support for repeat tries / grievance redressal to the customer. In addition to such information pertinent to an individual customer's AA journey, it would also be useful for the FIU to get anonymized, aggregated metadata about its customers' AA journey. Such metadata may include all information necessary for the FIU and the AA to jointly construct a "drop-off funnel" and use the same to improve user experience. The parameters that constitute such "metadata" are as defined here: https://sahamati.gitbook.io/aa-redirection-guidelines/v/1.2.1/specification/response-specification
Treatment	Mandatory
Published on	August 31, 2022
Modified on	February 23, 2024; June 11, 2025

Code of Conduct No.	CC037
Target audience	FIUs, AAs
Purpose	To clarify branding guidelines for co-designed AA Client screens
Description	All AA Client screens that are co-designed with FIUs ought to include "Powered by <AA Name>" along with an appropriate trust marker such as "<RBI registered entity>", in a clearly visible area of the screen. The AA Logo may be optionally added, next to the AA Name.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC038
Target audience	FIUs, AAs
Purpose	To clarify that the FIU name and logo should be displayed on AA Client screens in a *redirection* type of integration
Description	AA Client screens should show the FIU name and/or logo, from-and-to which the customer will be redirected. This is to enable contextual continuity to users while switching between the FIU and AA interfaces.
Treatment	Recommended
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC052
Target audience	AAs
Purpose	To clarify that all AAs must strictly adhere to the AA SDK Security Guidelines
Description	Sahamati has published a detailed set of AA SDK Security Guidelines to codify the minimum security requirements that all AAs must implement for their SDKs offered as AA Client for embedding third party apps, such as FIU apps. The AA SDK should be able to capture information securely without exposing the information captured to the embedding FIU app. Currently, the guidelines are available for Web and Android platforms, which are available below: ○ Guidelines for web based SDKs ○ Guidelines for Android platform based SDKs
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

Code of Conduct No.	CC039
Target audience	FIUs, AAs
Purpose	To clarify that all FIUs and AAs must strictly adhere to the AA Redirection Guidelines
Description	All FIUs and AAs must strictly adhere to the AA Redirection Guidelines, which are available at the below link: https://sahamati.gitbook.io/aa-redirection-guidelines
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

9. Customer Experience

Code of Conduct No.	CC053
Target audience	AAs
Purpose	To clarify the responsibility of AAs to keep customers informed regarding their consent(s) against which their financial data is being fetched on a recurring basis, such as through account monitoring consent(s)
Description	To ensure customers remain aware of their existing consents which permit FIUs to make recurring fetches of their financial data, AAs should, via appropriate communication channels, provide regular notifications to their customers regarding the data fetches made against such consent(s). AAs may appropriately implement such communications with the customers while upholding the spirit of this code.
Treatment	Mandatory
Published on	June 11, 2025
Modified on	N/A

Code of Conduct No.	CC040

Target audience	FIUs, AAs
Purpose	To clarify the recommended standards and design principles for customer experience design and user journeys within AA framework based on community-driven initiatives
Description	All FIUs and AAs should ensure that their customer experience design and user journeys within AA framework are aligned with the minimum standards and design principles outlined in the Sahamati-IDEO Design Report. This report lays out clear key design principles for: 1. The AA flow - Includes educating customers about Account Aggregators before AA Redirection, AA registration and login, as well as discovery and linking of financial accounts with AA account. 2. Informed Consent - Includes Consent Notice screens, Accept, and Reject flows, as well as Error and Success notification screens 3. Consent Revocation - Includes Consent Review/ Management screens, and Revocation screens The Sahamati-IDEO Design Report is available at the link below: https://sahamati.org.in/wp-content/uploads/2023/05/IDEO-LMM-Sahamati-Collab-on-AA-Flow-v1-compressed.pdf It should be noted that the principles underlying the above report should be adhered to in their spirit. All Sahamati Members and other participants should suitably adopt them in their user journeys. Entities should refer to the design principles underpinning the report which are consolidated at the below links: https://github.com/Sahamati/customer-experience-guidelines/blob/main/consent-guidelines.md Reference figma (screens) from the IDEO report is available here.
Treatment	Recommended
Published on	June 11, 2025
Modified on	N/A

CHAPTER IV

Codes of Conduct for FIPs

1. Account Discovery

Code of Conduct No.	CC044
Target audience	AAs, FIPs
Purpose	To clarify what are considered "Strong Identifiers" for Discovery and whether additional identifying attributes can be added to these
Description	As per ReBIT, (as given here) strong identifiers are one of the following: ● Mobile Number ● Email ID ● Aadhaar Number Additional identifiers, such as Date of Birth, PAN - can be added, as required by each FIP, as per ReBIT Circular No. ReBIT/AA/2024-25/01 dated January 10, 2024. All additional identifiers must be clubbed with the Strong Identifier value using an "AND" condition. The type of identifiers supported for discovery at an FIP's end are stored against each FIP's entry in the Central Registry.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	February 23, 2024; June 11, 2025

Code of Conduct No.	CC054
Target audience	FIPs
Purpose	To clarify that discovery of an account cannot be enabled by an FIP if the account status is NOT active

Code of Conduct No.	CC054
Description	If the status of a customer account is NOT active (i.e. it is either dormant or suspended or closed), it is in the interest of the customer for additional services (such as the sharing of account information) to NOT be authorised for discovery by the FIP.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	February 23, 2024

Code of Conduct No.	CC055
Target audience	FIPs
Purpose	To clarify if discovery of an account can be enabled by an FIP if the customer identifier (such as mobile number) does not resolve to a single customer record.
Description	If a mobile number does not resolve to a single customer record, the FIP is expected to reject the “Discovery” request. Additional identifying attributes (such as DOB, e.g.) may be defined by the FIP and collected by the AA, to sharpen the query and resolve it to a single customer record.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	N/A

2. Account Linking and delinking

Code of Conduct No.	CC056
Target audience	FIPs
Purpose	To clarify that the identifier used by an FIP to authenticate and authorise account linking need not be the same as the identifier used by the FIP for discovery.

Description	Discovery of an account at an FIP has to be on the basis of at least one STRONG identifier (mobile, email). An FIP may also require one or more additional identifiers (DOB, PAN, etc.) as per ReBIT Circular No. ReBIT/AA/2024-25/01 dated January 10, 2024. Account linking has to be authorised by an FIP on the basis of the account owner getting authenticated through an identifier that the FIP's records have. Currently, the authentication is through a single-factor. For all practical purposes, an identifier used for enabling a discovery call will be the same as that used to authenticate and authorise a linking request. However, strictly speaking, it is not necessary for these to be the same. It is possible, e.g. for a discovery call to happen via an email ID seeded in the FIP's records while linking may be authorised via a mobile number seeded in the FIP's records. Further, if and when multi-factor authentication becomes necessary to authorise linking, additional identifiers may be required to be sought during linking.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC057
Target audience	FIPs
Purpose	To clarify that de-linking of an account does not need the FIP's authorisation.
Description	No authentication or authorisation is needed to be performed by the FIP, when it receives a "Delink" instruction from the customer via the customer's AA.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

Code of Conduct No.	CC058
Target audience	FIPs
Purpose	To clarify that linking of accounts should not be authorised by an FIP if the account status is NOT active.
Description	If the status of an account is NOT active in the FIP's records (i.e. it is either dormant or suspended or closed), it is in the interest of the customer for additional services (such as the sharing of account information) to NOT be authorised by the FIP. Hence, linking of such an account should not be authorised.
Treatment	Mandatory
Published on	August 31, 2022
Modified on	February 23, 2024

3. Consent Lifecycle Management

Code of Conduct No.	CC021
Target audience	FIUs, FIPs
Purpose	To clarify the mechanism for a customer to *initiate* the process of revoking a consent via an FIU or an FIP channel, instead of directly on the AA interface.
Description	A customer should be able to initiate his/her intent to revoke a consent on an FIU or an FIP channel. Such a channel may be designed as per the FIU's or FIP's preference. The intent to revoke, once demonstrated to the FIU/ FIP by the customer, should result in the customer a. either being re-directed digitally to the AA that the customer has used previously, for the customer to complete the process of revocation b. Or alternatively, being provided information as to how the customer can independently invoke the AA's interface and complete the process of revocation. It is strongly recommended that FIUs and FIPs implement point (a) above, to enable ease for customers. In this context, ReBIT has clarified in its FAQs as follows:

	“FIP or FIU can use the POST /Consent/Notification API hosted by AA to raise a consent status update request to revoke consent. AA can perform the actual consent status update as per the request received after customer confirmation and notify FIP/FIU.”
Treatment	Mandatory
Published on	August 31, 2022
Modified on	June 11, 2025

4. FIP roles and responsibilities

Code of Conduct No.	CC059
Target audience	FIPs
Purpose	To clarify that an FIP can define the combination of identifiers it deems as “unique” for enabling identification of customers
Description	Each FIP can define the combination of identifiers it deems fit for it to uniquely identify an account owner and enable discovery of accounts. This definition is then expected to be made available by FIPs to all AAs through the Sahamati Central Registry, so that the AAs may collect the necessary attributes on their interface while enabling discovery and linking.
Treatment	Clarificatory
Published on	August 31, 2022
Modified on	June 11, 2025

****