Adoption Confirmation Report

(To be submitted by Account Aggregators and Financial Information Users to ReBIT once the AA client-side application adoption is completed. The document should be sent to ***aa-apirelease@rebit.org.in*** *with a cc to* ***cgmfintech@rbi.org.in****)*

To,

ReBIT Fintech Team
Reserve Bank Information Technology Private Limited

Subject: NBFC-AA Client Standards Adoption Confirmation Report

Respected Sir/Madam,

This is with reference to the above-mentioned subject; We hereby confirm that we have adopted the latest version **1.0.0** of the AA client-side applications on yyyy-mm-dd as specified in *"Standards to Enhance Customer Protection and User Experience within the Account Aggregator Framework."*

Table 1: Entity Details		
1	Name of the Entity	Enter Entity Name
2	Type of the Entity	-Choose an item-
3	Regulator	-Choose an item-
4	Authorized Official Name	Enter Authorized Official Name
5	Authorized Official Designation	Enter Authorized Official Designation
6	Authorized Official Email	Enter Authorized Official Email
7	Authorized Official Contact Number	Enter Authorized Official Contact Number

We, Enter Entity Name certify that the particulars given above are true and correct to the best of our knowledge and belief.

Place: Enter place
Date: yyyy-mm-dd

<<Sign>>

Authorized Official

(Head of technology strategy or above)

Name: Enter Authorized Official Name
Designation: Enter Authorized Official Designation

Annexure:

1. Checklist to be submitted by Account Aggregator and Financial Information Users (FI-Us) entities:

Table 3: Standards (as applicable to AA/FI-U)				
S.No.	**Points to be Implemented**	**Mandatory / Optional**	**Applicability**	**Compliance Status (Yes/No)**
1.	Customer can link up to two mobile numbers for account discovery	Mandatory	-Choose an item-	-Choose an item-
2.	Optional identifiers (PAN / Date of Birth) for account discovery	Mandatory	-Choose an item-	-Choose an item-
3.	Authentication required for account delinking; ensure active consents revoked	Mandatory	-Choose an item-	-Choose an item-
4.	Customer profile captures minimum details (Name, Verified Mobile, Email) with masking	Optional	-Choose an item-	-Choose an item-
5.	Virtual User Address (VUA) provided as unique identifier	Mandatory	-Choose an item-	-Choose an item-
6.	AA Client checks if account already exists before onboarding	Mandatory	-Choose an item-	-Choose an item-
7.	Account closure facility with revocation of active consents and delinking of accounts	Mandatory	-Choose an item-	-Choose an item-
8.	Account recovery facility (digital/manual) with mobile verification	Mandatory	-Choose an item-	-Choose an item-
9.	Clear presentation of consent fields (Start, Expiry, Fetch Type, FI Types, FI-U, Purpose, Data Range, Frequency)	Mandatory	-Choose an item-	-Choose an item-
10.	Remaining consent fields shown via “View More”	Mandatory	-Choose an item-	-Choose an item-
11.	Voice-based reading of consent parameters	Optional	-Choose an item-	-Choose an item-
12.	Approve/Reject buttons equal size and visibility, no default pre-selection	Mandatory	-Choose an item-	-Choose an item-
13.	Separate Approve/Reject for multiple consents	Mandatory	-Choose an item-	-Choose an item-
14.	Consent expiry mechanisms implemented	Mandatory	-Choose an item-	-Choose an item-
15.	Explicit account selection for consent approval (opt-in, no preselection)	Mandatory	-Choose an item-	-Choose an item-
16.	Consent Dashboard showing active consents and data fetch history	Mandatory	-Choose an item-	-Choose an item-

17.	Tamper-proof audit trail of consent activities	Mandatory	-Choose an item-	-Choose an item-
18.	Immutable consent artefacts	Mandatory	-Choose an item-	-Choose an item-
19.	Robust security practices for consent (encryption, access controls, audits)	Mandatory	-Choose an item-	-Choose an item-
20.	Simple and user-friendly design of AA Client	Mandatory	-Choose an item-	-Choose an item-
21.	Accessibility compliance (WCAG 2.0, alt text, contrast)	Mandatory	-Choose an item-	-Choose an item-
22.	Multi-language support	Mandatory	-Choose an item-	-Choose an item-
23.	FI-P list visible to customers	Mandatory	-Choose an item-	-Choose an item-
24.	Usability testing and feedback mechanisms	Mandatory	-Choose an item-	-Choose an item-
25.	FI-U informs users about redirection to AA Client	Optional	-Choose an item-	-Choose an item-
26.	AA Client displays name/logo prominently	Mandatory	-Choose an item-	-Choose an item-
27.	Tagline "RBI Regulated NBFC-AA" displayed	Optional	-Choose an item-	-Choose an item-
28.	Real-time notifications for account linking, consent approvals/revocations	Mandatory	-Choose an item-	-Choose an item-
29.	Monthly SMS/email updates on active consents and data fetches	Mandatory	-Choose an item-	-Choose an item-
30.	FI-U provides data fetch summaries with customizable frequency	Optional	-Choose an item-	-Choose an item-
31.	Users can customize notification preferences	Mandatory	-Choose an item-	-Choose an item-
32.	Two-Factor Authentication (2FA) implemented	Mandatory	-Choose an item-	-Choose an item-
33.	SIM and device binding for mobile apps	Mandatory	-Choose an item-	-Choose an item-
34.	Browser fingerprinting for web apps	Mandatory	-Choose an item-	-Choose an item-
35.	CERT-In audit before production release and major updates	Mandatory	-Choose an item-	-Choose an item-
36.	Annual security assessments	Mandatory	-Choose an item-	-Choose an item-
37.	Compliance with industry standards and regulations	Mandatory	-Choose an item-	-Choose an item-
38.	Secure integration methods (Deep Linking, Redirection, SDK, iFrame)	Mandatory	-Choose an item-	-Choose an item-
39.	Strong mutual authentication and encryption in integrations	Mandatory	-Choose an item-	-Choose an item-
40.	Responsibilities defined when providing SDK	Mandatory	-Choose an item-	-Choose an item-
41.	FI-U performs due diligence of AA SDK	Mandatory	-Choose an item-	-Choose an item-
42.	AA Client allows users to view/download financial data with explicit consent	Optional	-Choose an item-	-Choose an item-

43.	Data decrypted locally on customer device only	Mandatory	-Choose an item-	-Choose an item-
44.	Downloaded files masked, password-protected, watermarked	Mandatory	-Choose an item-	-Choose an item-
45.	Compliance with DPDP Act, 2023	Mandatory	-Choose an item-	-Choose an item-
46.	Secure communication protocols (TLS v1.2+)	Mandatory	-Choose an item-	-Choose an item-
47.	Secure API integrations with authentication, authorization, input validation	Mandatory	-Choose an item-	-Choose an item-
48.	Certificate pinning or equivalent measures	Mandatory	-Choose an item-	-Choose an item-
49.	Robust encryption for sensitive data at rest/in transit	Mandatory	-Choose an item-	-Choose an item-
50.	Secure key management practices	Mandatory	-Choose an item-	-Choose an item-
51.	Secure coding practices (input validation, output encoding, protection against XSS, injection)	Optional	-Choose an item-	-Choose an item-
52.	Regular code reviews and security audits	Mandatory	-Choose an item-	-Choose an item-
53.	Comprehensive testing (functional, security, performance, compatibility)	Mandatory	-Choose an item-	-Choose an item-
54.	Automated testing frameworks and CI practices	Optional	-Choose an item-	-Choose an item-
55.	Robust error handling without exposing debug logs	Mandatory	-Choose an item-	-Choose an item-
56.	Logging with masked sensitive data	Optional	-Choose an item-	-Choose an item-
57.	Due diligence on third-party libraries/SDKs	Mandatory	-Choose an item-	-Choose an item-
58.	Remote access disabled for mobile app	Mandatory	-Choose an item-	-Choose an item-
59.	Rooted/jailbroken devices blocked	Mandatory	-Choose an item-	-Choose an item-
60.	Secure push notifications	Mandatory	-Choose an item-	-Choose an item-
61.	Runtime Application Self-Protection (RASP)	Mandatory	-Choose an item-	-Choose an item-
62.	Re-authentication after inactivity	Mandatory	-Choose an item-	-Choose an item-
63.	Software Bill of Materials (SBOM) maintained	Optional	-Choose an item-	-Choose an item-
64.	Compatibility with latest Android/iOS versions	Mandatory	-Choose an item-	-Choose an item-
65.	Regular updates for platform features/security patches	Mandatory	-Choose an item-	-Choose an item-
66.	Version governance to phase out old versions	Mandatory	-Choose an item-	-Choose an item-
67.	Public checksum of active version hosted	Optional	-Choose an item-	-Choose an item-

68.	Web app input validation and output encoding	Mandatory	-Choose an item-	-Choose an item-
69.	Web app performance optimization (loading times, caching)	Optional	-Choose an item-	-Choose an item-
70.	Use of CDNs for performance	Optional	-Choose an item-	-Choose an item-
71.	Cross-browser compatibility testing	Mandatory	-Choose an item-	-Choose an item-
72.	Mobile SDK robust authentication mechanisms	Mandatory	-Choose an item-	-Choose an item-
73.	OAuth 2.0 for authorization	Optional	-Choose an item-	-Choose an item-
74.	Secure token management (refresh, invalidate)	Mandatry	-Choose an item-	-Choose an item-
75.	Secure storage (Keychain/Keystore)	Optional	-Choose an item-	-Choose an item-
76.	Access controls restricting SDK data access	Mandatory	-Choose an item-	-Choose an item-
77.	Encryption of SDK payloads	Optional	-Choose an item-	-Choose an item-
78.	Regular vulnerability scans and patches for SDK	Mandatory	-Choose an item-	-Choose an item-
79.	Secure integration mechanisms (API keys, client certificates)	Mandatory	-Choose an item-	-Choose an item-
80.	Security testing (penetration, code reviews)	Mandatory	-Choose an item-	-Choose an item-
81.	Rooted/jailbroken devices blocked for SDK	Mandatory	-Choose an item-	-Choose an item-
82.	Comprehensive SDK documentation	Mandatory	-Choose an item-	-Choose an item-
83.	Developer support channels available	Mandatory	-Choose an item-	-Choose an item-
84.	Adherence to Android/iOS guidelines	Mandatory	-Choose an item-	-Choose an item-
85.	Regular SDK updates	Mandatory	-Choose an item-	-Choose an item-
86.	PKI for sensitive data (OTPs, PINs, passwords)	Optional	-Choose an item-	-Choose an item-
87.	PKI digital signatures for authenticity/integrity	Optional	-Choose an item-	-Choose an item-
88.	SIM binding via outgoing SMS + OTP auto-read	Mandatory	-Choose an item-	-Choose an item-
89.	Device binding via unique identifiers	Mandatory	-Choose an item-	-Choose an item-
90.	Browser fingerprinting for web apps	Mandatory	-Choose an item-	-Choose an item-
91.	Session security with device-bound tokens	Mandatory	-Choose an item-	-Choose an item-
92.	Strong encryption of device identifiers	Mandatory	-Choose an item-	-Choose an item-
93.	Mandatory mobile data during binding	Mandatory	-Choose an item-	-Choose an item-
94.	Restriction on app toggling during binding	Mandatory	-Choose an item-	-Choose an item-
95.	Fallback authentication for SIM/device changes	Mandatory	-Choose an item-	-Choose an item-
96.	Device visibility for customers	Mandatory	-Choose an item-	-Choose an item-
97.	Limit on number of device bindings per user	Mandatory	-Choose an item-	-Choose an item-

98.	Deep Linking integration (URL schema, Intents, Universal Links, secure tokens, fallback, user choice)	Mandatory	-Choose an item-	-Choose an item-
99.	Secure SDK integration with FI-U apps	Mandatory	-Choose an item-	-Choose an item-
100.	Secure iFrame integration with AA Web App	Mandatory	-Choose an item-	-Choose an item-
101.	Secure redirection with FI-U Web App	Mandatory	-Choose an item-	-Choose an item-

Validate

Reset