INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 5 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 5 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-5-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

INDIA'S ACCOUNT AGGREGATOR FRAMEWORK: LEGAL ARCHITECTURE FOR DATA PROTECTION AND CONSENT MANAGEMENT

AUTHOR - SHRUTI KESARWANI* & DR ARVIND P. BHANU**

* STUDENT OF LAW, AMITY LAW SCHOOL, NOIDA UTTAR PRADESH

** FACULTY OF LAW, AMITY LAW SCHOOL, NOIDA UTTAR PRADESH

BEST CITATION - SHRUTI KESARWANI & DR ARVIND P. BHANU, THE BLACK BOX OF AI: WHO'S TO BLAME?, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 5 (5) OF 2025, PG. 906-914, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

This paper examines India's Account Aggregator (AA) framework, a novel financial data-sharing ecosystem that facilitates secure and consent-based exchange of financial information between "Financial Information Providers (FIPs)" and "Financial Information Users (FIUs)". The research analyzes the legal and regulatory framework underpinning the AA ecosystem, with particular emphasis on data protection mechanisms, consent architecture, and security requirements. The Digital Personal Data Protection Act, 2023 (DPDP Act)[1776] has significantly strengthened the legal foundation of the AA framework by establishing robust provisions for data protection, consent management, and enforcement mechanisms. This paper investigates how the interplay of various regulations shapes the functioning of AAs as intermediaries in financial data sharing while ensuring user privacy and data security. The research concludes that while India's AA framework represents a progressive approach to consent-based data sharing, several challenges regarding implementation standardization, technological barriers, and regulatory coordination remain to be addressed for the framework to achieve its full potential.

1776 The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

1. Introduction

India's financial landscape has witnessed significant digital transformation in recent years, with the Account Aggregator (AA) framework emerging as a pivotal innovation in financial data sharing. This framework represents a paradigm shift from traditional methods of financial information exchange by establishing a regulated, consent-driven ecosystem for seamless data flow between financial institutions. As financial services increasingly migrate to digital platforms, the need for secure, efficient, and user-controlled sharing of financial information has become paramount.

The AA framework, conceptualized and regulated by the Reserve Bank of India (RBI), addresses this need by creating a class of Non-Banking Financial Companies (NBFCs) that function as intermediaries facilitating the flow of financial data between Financial Information Providers (FIPs) and Financial Information Users (FIUs). [1777] The framework's distinctive feature lies in its consent-centric approach, empowering individuals with complete control over their financial information while enabling them to leverage this data for accessing various financial services.

With the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), India's data protection regime has undergone a significant transformation, providing a more robust legal foundation for consent-based data sharing frameworks like the AA ecosystem. The DPDP Act establishes comprehensive provisions for data protection, consent management, and enforcement mechanisms that complement and strengthen the regulatory framework governing AAs.[1778]

This research paper aims to analyze the legal architecture underpinning India's AA framework, with particular focus on data protection and consent management mechanisms. The study examines how various legislative and regulatory instruments interact to create a secure, transparent, and user-controlled ecosystem for financial data sharing, while also identifying challenges and limitations that need to be addressed for the framework to achieve its full potential.

2. Research Methodology

This study employs doctrinal legal research methodology, focusing on an analytical examination of primary and secondary legal sources related to India's Account Aggregator framework. The research primarily analyzes legislative texts, regulatory directives, and policy frameworks that govern data protection and consent architecture in the AA ecosystem.

The primary sources examined include:

- The Digital Personal Data Protection Act, 2023[1779]
- The Information Technology Act, 2000[1780]
- RBI Master Directions on NBFC-Account Aggregators, 2016 [1781]
- Sectoral regulations issued by SEBI, IRDAI, and PFRDA
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[1782]

These sources were systematically analyzed to understand the legal requirements governing data classification, consent mechanisms, security standards, and liability frameworks within the AA ecosystem. The research adopts a descriptive-analytical approach to elucidate how these legal provisions interact to create a

1777 "RBI Master Direction -Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016" issued on September 2, 2016" *available at*:

"https://m.rbi.org.in//scripts/BS_ViewMasDirections.aspx?id=10598 (last visited March 30, 2025)."

1778 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 2. "

1779 *Supra* Note 1 at 1.

1780 "The Information Technology Act, 2000 (Act No. 21 of 2000)."

1781 *Supra* Note 2 at 1.

1782 "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, No. G.S.R. 313(E), Ministry of Communications and Information Technology, Govt. of India." *Available at- https://prsindia.org/billtrack/the-information-technology-rules-2011 (last visited March 30, 2025)."*

comprehensive regulatory framework for data protection in financial information sharing.

The methodology also incorporates a comparative analysis of how different sectoral regulators approach data protection within their respective domains, providing insights into the multi-layered regulatory structure of the AA framework. This research does not involve empirical data collection but relies on interpretative analysis of legal texts and regulatory frameworks.

3. Legal Framework for Data Protection in the AA Ecosystem

3.1 Legislative Foundation

The Account Aggregator ecosystem in India operates within a complex legal environment comprising multiple legislative and regulatory instruments. At the core of this framework lies the Digital Personal Data Protection Act, 2023 (DPDP Act), which establishes fundamental principles of data protection applicable to financial information sharing.[1783] The Act supersedes previous frameworks and introduces principles of data minimization, purpose limitation, and user consent that align perfectly with the AA framework's consent-based design.

Section 4 of the DPDP Act requires that personal data be processed only for legitimate purposes and with the intention or consent of the data principal.[1784] This provision forms the legal backbone of the consent-driven approach of the AA ecosystem. Furthermore, Section 6 reinforces purpose limitation, ensuring that data collected under the AA framework may only be used for the specific financial purpose for which consent has been explicitly provided.

Supplementing the DPDP Act is the Information Technology Act, 2000 (IT Act)[1785], which provides the legal framework for electronic data protection. Section 43A of the IT Act mandates reasonable security practices for organizations handling sensitive personal data, including financial information.[1786] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, further categorize financial information as "sensitive personal data," imposing additional security obligations on FIPs and FIUs operating within the AA ecosystem.[1787]

3.2 Regulatory Framework

The Reserve Bank of India's Master Directions on NBFC-Account Aggregators, 2016, issued under Section 45-IA of the Reserve Bank of India Act, 1934, establish the sectoral regulatory framework specifically governing Account Aggregators.[1788] These Directions define AAs as regulated entities that facilitate consent-based data sharing but are prohibited from storing or processing financial data except for the purpose of securely transmitting it between FIPs and FIUs.

The regulatory framework extends beyond banking to encompass other financial sectors through sectoral regulations issued by various authorities:

1. The IRDAI has issued circulars and guidelines governing the processing of policyholder information in the insurance industry. The IRDAI (Protection of Policyholders' Interests) Regulations, 2017, mandate robust data protection controls for insurers sharing policyholder information through AAs.[1789]

2. The SEBI regulates investment-related financial information through the SEBI (Investment Advisers) Regulations, 2013, and the SEBI (Portfolio Managers) Regulations, 2020.[1790] [1791]These regulations require investment advisers and portfolio managers to obtain express client

1783 *Supra* Note 1 at 1.
1784 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 4. "
1785 *Supra* Note 5 at 2.
1786 "The Information Technology Act, 2000 (Act No. 21 of 2000).s. 43"
1787 *Supra* Note 7 at 2.
1788 *Supra* Note 2 at 1.
1789 "Insurance Regulatory and Development Authority of India (Protection of Policyholders' Interests) Regulations, 2017."
1790 "Securities and Exchange Board of India (Investment Advisers) Regulations, 2013."
1791 "Securities and Exchange Board of India (Portfolio Managers) Regulations, 2020"

consent before accessing financial data, reinforcing the AA framework's consent-based model.

3. The PFRDA Guidelines establish data protection standards for pension fund administrators and National Pension System subscribers.[1792] The PFRDA (Point of Presence) Regulations, 2018[1793], prescribe consent-based access to financial data, aligning with the AA ecosystem's principles.

This multi-layered regulatory approach ensures comprehensive governance of financial data sharing across different sectors while maintaining consistency in core principles of consent, privacy, and security.

4. Classification of Financial Data in the AA Framework

4.1 Categories of Financial Information

The Account Aggregator framework adopts a nuanced approach to financial data classification, recognizing that different types of financial information warrant varying levels of protection based on their sensitivity and potential risk. The classification system is anchored in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, and further refined by the DPDP Act, 2023.

Financial information within the AA ecosystem is categorized into four primary types:

1. **Sensitive Financial Data**: This category encompasses information that, if compromised, could pose significant risks to an individual's financial security and privacy. It includes bank account information, credit and debit card numbers, transaction histories, and financial account passwords. Section 2 of the IT (Reasonable Security Practices) Rules identifies such data as sensitive, requiring robust security measures.[1794]. In the AA context, sensitive financial information receives the highest level of protection, with stringent encryption and access control requirements.

2. **Non-Sensitive Financial Information**: This category includes financial data that does not inherently compromise privacy or security if disclosed, such as salary information typically shared for loan applications or creditworthiness assessments. While not as heavily protected as sensitive financial data, this information still falls under the purview of the DPDP Act, 2023, and requires appropriate safeguards including encryption and restricted access.[1795]

3. **Transactional Data**: This category encompasses records of financial transactions such as purchases, payments, and transfers. In the AA model, transactional information flows between FIPs and FIUs through AAs with the explicit consent of customers. The RBI Master Directions mandate that entities handling such data implement strict access controls and encryption to protect against unauthorized disclosure.

4. **Anonymized Data**: This category refers to financial information stripped of personal identifiers, rendering it impossible to trace back to specific individuals. Under Section 16 of the DPDP Act, anonymized data may be used for statistical or research purposes without violating individual privacy rights.[1796] However, entities dealing with anonymized data in the AA framework must ensure that such data cannot be re-identified through technical or other means.

4.2 Regulatory Implications of Data Classification

The classification of financial data directly influences the regulatory requirements applicable to its processing within the AA ecosystem. Sensitive financial data is subject to

1792 "Pension Fund Regulatory and Development Authority (Aggregator) Regulations, 2015."
1793 "Pension Fund Regulatory and Development Authority (Point of Presence) Regulations, 2018".
1794 "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, s. 2"
1795 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 6."
1796 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 16."

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 5 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

the most stringent controls, including advanced encryption, multi-factor authentication, and comprehensive audit trails. Non-sensitive financial information, while requiring protection, may be subject to relatively less intensive security measures.

The RBI Master Directions specifically mandate that AAs implement tiered security protocols based on data sensitivity, ensuring proportionate protection measures across different categories of financial information. This risk-based approach to data protection aligns with global best practices while ensuring that compliance requirements remain practical and implementable.

5. Consent Architecture in the AA Framework

5.1 Legal Requirements for Consent Mechanisms

Consent forms the cornerstone of the Account Aggregator framework, with comprehensive legal parameters governing how consent is sought, managed, and withdrawn. The DPDP Act, 2023, together with the RBI Master Directions, establishes a robust legal foundation for consent mechanisms in financial data transactions facilitated by AAs.

Section 8 of the DPDP Act stipulates that consent must be freely given, specific, informed, and unambiguous.[1797] In the AA context, this translates to requirements that individuals must be fully aware of what financial information will be shared, for what purposes, and with which parties. General or implied consent is insufficient; explicit, recorded consent is mandatory before any financial information can be shared between FIPs and FIUs.

The principle of informed consent is codified in Section 11 of the DPDP Act, requiring entities to provide data subjects with clear, easily understandable information about data processing.[1798] This includes details about the purpose of data collection, retention periods, and potential risks associated with data sharing. In the AA ecosystem, this requirement materializes as transparent consent management frameworks that allow users to review and authorize the sharing of their financial data in comprehensible terms.

5.2 Electronic Consent Artifacts

Electronic Consent Artifacts (e-consent artifacts) represent a crucial innovation in the AA ecosystem, serving as digital evidence of an individual's consent to share financial data. These artifacts receive legal recognition under both data protection and financial regulations, making them verifiable and enforceable as proof of consent.

Section 8 of the DPDP Act requires that electronic consent be explicit, informed, and clear, with consent artifacts serving as evidence that individuals have authorized data sharing.[1799] The RBI-regulated AA framework mandates that each data sharing request be accompanied by an electronic consent artifact, ensuring transparency and adherence to data protection principles.

The IT Act, 2000, through Section 4, extends legal recognition to electronic records, ensuring that digitally signed consent artifacts hold the same validity as conventional written consent forms.[1800]Furthermore, Section 5 of the Act confers legal validity to electronic signatures, enabling consent artifacts to be rendered tamper-proof and verifiable.[1801]

5.3 Consent Withdrawal and Revocation

The right to withdraw consent represents a fundamental aspect of data autonomy within the AA framework. Section 9 of the DPDP Act establishes that consent is revocable at any time, requiring data fiduciaries, including AAs, to cease processing personal data upon such withdrawal.[1802] This provision ensures that users

1797 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 8".
1798 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 11."
1799 *Supra* Note 22 at 5.
1800 "The Information Technology Act, 2000 (Act No. 21 of 2000).s. 4."
1801 "The Information Technology Act, 2000 (Act No. 21 of 2000).s. 5."
1802 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 9."

are not indefinitely bound by previously granted consent.

The RBI Master Directions reinforce this principle by mandating easy-to-use revocation mechanisms within the AA framework. AAs must provide user interfaces with consent dashboards that allow individuals to monitor, manage, and withdraw consents in real-time, ensuring transparency and user control over data sharing arrangements.[1803]

Technologically, consent withdrawal triggers immediate notifications to relevant FIPs and FIUs, making revocation effective across all parties. Section 8 of the DPDP Act requires data fiduciaries to cease processing and delete data upon consent withdrawal, except where legal obligations require retention, protecting individuals from unauthorized continued use of their financial information.[1804]

6. Security Standards and Technical Requirements

6.1 Encryption and Data Protection Measures

The AA framework mandates robust security measures to protect financial information throughout its lifecycle. Section 24 of the DPDP Act requires all entities processing personal data, including AAs, FIPs, and FIUs, to implement appropriate security practices to safeguard against unauthorized access, use, or data breaches.[1805] This aligns with the Information Technology (Reasonable Security Practices and Procedures) Rules, 2011, which mandate encryption, access controls, and risk assessment protocols.

The RBI Master Directions specifically require AAs to implement end-to-end encryption when transmitting financial data, following internationally recognized cryptographic standards to prevent interception or alteration during transmission.[1806] Additionally, Section 43A of the IT Act holds organizations liable for compensation in cases of negligence leading to unauthorized data disclosure, incentivizing the implementation of best practices such as multi-factor authentication and regular security audits.[1807]

6.2 Data Localization Requirements

Data localization provisions under Section 15 of the DPDP Act stipulate that certain categories of sensitive financial information must be stored within India.[1808] This requirement enables regulatory oversight and enhanced security measures while reducing risks associated with cross-border data movement. The RBI's Guidelines on Data Localization further require that financial data processed within India's banking ecosystem be stored domestically, adding another layer of regulatory oversight for AAs.

6.3 Security Breach Notification and Liability

The legal framework establishes comprehensive requirements for security breach notification and liability within the AA ecosystem. Section 25 of the DPDP Act obligates data fiduciaries, including AAs, FIPs, and FIUs, to notify the Data Protection Board of India and affected individuals in the event of personal data breaches.[1809] Such notifications must include information about the nature of the breach, types of data affected, potential harms, and remedial actions being undertaken.

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions) Rules, 2013, require financial institutions, including AAs, to report cybersecurity incidents to CERT-In within six hours of discovery. This rapid reporting requirement ensures prompt response to security breaches, minimizing potential damage to affected individuals.

1803 *Supra* Note 2 at 1.
1804 *Supra* Note 22 at 5.
1805 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 24."
1806 *Supra* Note 2 at 1.
1807 "The Information Technology Act, 2000 (Act No. 21 of 2000).s. 43A."
1808 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 15."
1809 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 25."

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Section 21 of the DPDP Act provides that individuals affected by data breaches resulting in financial loss or identity theft have the right to claim compensation from responsible data fiduciaries.[1810] The Data Protection Board of India can impose monetary penalties on financial institutions failing to meet security requirements, ensuring accountability and incentivizing robust security practices.

7. Challenges and Limitations in the AA Framework

7.1 Regulatory Coordination Challenges

The multi-regulator landscape governing the AA ecosystem presents significant coordination challenges. While the RBI serves as the primary regulator for AAs, financial data flows across sectors regulated by different authorities including SEBI, IRDAI, and PFRDA. This fragmentation can lead to inconsistent implementation of data protection standards and potential regulatory gaps.

Each sectoral regulator has developed its own guidelines and standards for data protection, which, while generally aligned with the principles of the DPDP Act, may differ in specific requirements and enforcement mechanisms. This regulatory complexity increases compliance costs for AAs operating across multiple financial sectors and may create uncertainty regarding applicable standards in edge cases.

The establishment of the Data Protection Board under the DPDP Act presents an opportunity to harmonize these regulatory approaches, but effective coordination mechanisms between the Board and sectoral regulators remain to be developed. Without robust coordination frameworks, there is a risk of regulatory overlap or contradictory requirements that could undermine the efficiency of the AA ecosystem.

7.2 Technical Implementation Challenges

The AA framework's heavy reliance on technology for consent management, data encryption, and secure transmission introduces several technical challenges:

1. **Interoperability Issues**: Different FIPs and FIUs may implement varying technical standards for data formats, encryption protocols, and authentication mechanisms, potentially hindering seamless data flow through AAs. While the RBI has prescribed certain technical standards, achieving full interoperability across the financial ecosystem remains challenging.

2. **Security Vulnerabilities**: The complex technical architecture of the AA ecosystem creates multiple potential attack vectors for malicious actors. Ensuring consistent security standards across all participants in the ecosystem requires continuous monitoring, updating, and testing of security protocols.

3. **User Interface Limitations**: The effectiveness of consent mechanisms largely depends on user-friendly interfaces that clearly communicate data sharing parameters to individuals. Current implementations may not adequately address varying levels of digital literacy among users, potentially undermining informed consent.

7.3 Awareness and Adoption Barriers

Despite its innovative approach to financial data sharing, the AA framework faces significant challenges related to user awareness and adoption:

1. **Limited Public Understanding**: The concept of consent-based data sharing through AAs remains relatively unfamiliar to many Indians, particularly in semi-urban and rural areas. Without adequate awareness, individuals may be hesitant to utilize AA services or may not fully understand the implications of their consent decisions.

2. **Trust Deficit**: Given the sensitive nature of financial information, building public trust in

1810 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023). s. 21."

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 5 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

the AA ecosystem is crucial for widespread adoption. Recent data breaches in various sectors have heightened public concerns about data security, potentially deterring adoption of new data-sharing mechanisms.

3. **Digital Divide**: The AA framework's reliance on digital interfaces for consent management may exclude populations with limited digital access or literacy, potentially exacerbating financial exclusion for already marginalized groups.

8. Conclusion and Suggestions

8.1 Conclusion

India's Account Aggregator framework represents a pioneering approach to consent-based financial data sharing, establishing a regulated ecosystem that balances innovation with privacy protection. The framework's legal architecture, anchored in the DPDP Act, 2023[1811], and supplemented by sectoral regulations, provides a comprehensive foundation for secure, transparent, and user-controlled financial data sharing.

The AA framework's distinctive features—explicit consent requirements, electronic consent artifacts, robust withdrawal mechanisms, and stringent security standards—collectively establish a progressive model for data protection in financial services. By empowering individuals with control over their financial information while enabling its beneficial use, the framework aligns with evolving global standards for data protection while addressing India-specific requirements.

However, significant challenges remain in realizing the full potential of the AA ecosystem. Regulatory fragmentation, technical implementation hurdles, and adoption barriers necessitate continued refinement of the framework. The success of the AA ecosystem will ultimately depend on addressing these challenges while maintaining its core principles of user control, security, and transparency.

8.2 Suggestions

Based on the analysis conducted in this research, the following recommendations are proposed to strengthen the AA framework:

1. **Establish a Cross-Regulatory Coordination Mechanism**: Create a formal coordination committee comprising representatives from the RBI, SEBI, IRDAI, PFRDA, and the Data Protection Board to harmonize data protection standards and enforcement mechanisms across financial sectors. This would reduce regulatory fragmentation and ensure consistent implementation of the AA framework.

2. **Develop Standardized Technical Protocols**: The RBI, in collaboration with industry stakeholders, should develop comprehensive technical standards covering data formats, encryption protocols, and authentication mechanisms to enhance interoperability within the AA ecosystem. These standards should be regularly updated to address emerging security threats and technological advancements.

3. **Enhance User Interface Requirements**: Establish minimum standards for consent dashboards and management interfaces to ensure clarity, accessibility, and usability across different demographic segments. These standards should address varying levels of digital literacy and potentially include vernacular language support.

4. **Implement Tiered Consent Models**: Develop and standardize tiered consent models that allow individuals to grant access to different categories of financial information with varying levels of granularity, enhancing user control while simplifying the consent process for common use cases.

5. **Launch Public Awareness Campaigns**: Regulatory authorities should collaborate with industry associations to conduct comprehensive public awareness campaigns explaining the benefits, safeguards, and functioning of the AA ecosystem. These campaigns should target diverse demographic

1811 "The Digital Personal Data Protection Act, 2023 (Act No. 30 of 2023)."

segments using appropriate communication channels.

6. **Establish Specialized Dispute Resolution Mechanisms**: Create specialized forums or processes for resolving disputes related to unauthorized data sharing, consent violations, or security breaches within the AA ecosystem. These mechanisms should provide expedited resolution while ensuring accessibility for all users.

7. **Conduct Regular Security Audits**: Mandate regular independent security audits for all participants in the AA ecosystem, with results reported to regulatory authorities. These audits should assess compliance with prescribed security standards and identify potential vulnerabilities for remediation.

8. **Develop Privacy-Enhancing Technologies**: Encourage research and development of privacy-enhancing technologies specifically designed for the AA ecosystem, such as advanced encryption methods, privacy-preserving analytics, and secure multi-party computation techniques.

By implementing these recommendations, India can further strengthen its Account Aggregator framework, addressing current limitations while building on its innovative foundation to create a truly world-class ecosystem for consent-based financial data sharing.

Bibliography

Statutes and Regulations

1. Digital Personal Data Protection Act, 2023.
2. Information Technology Act, 2000.
3. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
4. Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions) Rules, 2013.
5. Insurance Regulatory and Development Authority of India (Protection of Policyholders' Interests) Regulations, 2017.
6. Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017.
7. National Cyber Security Policy, 2013.
8. Pension Fund Regulatory and Development Authority (Point of Presence) Regulations, 2018.
9. Pension Fund Regulatory and Development Authority (Aggregator) Regulations, 2015.
10. Reserve Bank of India, Master Directions on NBFC-Account Aggregators, 2016.
11. Securities and Exchange Board of India (Investment Advisers) Regulations, 2013.
12. Securities and Exchange Board of India (Portfolio Managers) Regulations, 2020.
13. SEBI Cyber Security and Cyber Resilience Framework.

Secondary Sources

1. Bhattacharya, Rahul & Raj Singh. "The Account Aggregator Framework: Reimagining Financial Data Sharing in India." 17 J. Banking Reg. 243 (2022).
2. Chandrasekhar, Ravi. "Digital Personal Data Protection Act, 2023: A Commentary." 56 Econ. & Pol. Wkly. 32 (2023).
3. D'Silva, Sinclair, et al. "The Design of Digital Financial Infrastructure: Lessons from India." BIS Paper No. 106 (2019).
4. Gupta, Anurag. "Data Protection in Financial Services: Emerging Frameworks and Challenges." 15 Int'l J. L. & Info. Tech. 127 (2023).
5. Jain, Prashant. "Consent Architecture for Financial Information Sharing: The

Account Aggregator Model." 42 Comp. L. & Sec. Rev. 108 (2021).

6. Khaitan, Tarunabh. "India's Privacy Law: The Digital Personal Data Protection Act, 2023." 86 Mod. L. Rev. 459 (2024).
7. Matthan, Rahul. "The Privacy Law: A Framework for the Future." 5 Indian J. L. & Tech. 118 (2023).
8. Padmanabhan, Geeta. "Account Aggregators: Changing the Landscape of Financial Data Sharing." RBI Bulletin (March 2022).
9. Prasad, Amber. "Security Standards for Financial Data Protection in India." 37 J. Fin. Crime 215 (2023).
10. Reserve Bank of India. "Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps." (November 2021).
11. Saraf, Niharika & Anupam Manur. "Account Aggregator: Transforming Financial Services Through Data Sharing." Takshashila Institution Working Paper (2021).