JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Open Finance, Divergent Paths: A Regulatory Design Comparison of India's Account Aggregator, PSD2, and Australia's Consumer Data Right

Submitted by:
Nimisha Thakkar
MBA (Banking and Finance), Semester IV
Amity Business School, Amity University Mumbai, India

Under the Guidance of:
Prof. Shija Abhilash
Amity Business school, Amity University Mumbai, India.

Abstract: The global developments in the regulation of Open Finance have resulted in the emergence of different regulatory architectures, shaped by varying underpinning philosophies on data governance, empowering consumers, and market structures. This study undertakes a systematic comparative analysis of three different Open Finance regulatory architectures: the Account Aggregator model in India, the Second Payment Services Directive in the European Union, and the Consumer Data Right in Australia, using five parameters: the consent model, mandatory participation, liability allocation, interoperability standards, and enforcement mechanisms. The Account Aggregator model in India, which has achieved 252.9 million user accounts and a cumulative loan disbursement of Rs 1.3 lakh crore as of early 2026, after its implementation in September 2021 and its identification as Digital Public Infrastructure in 2023, is challenged in the areas of the quality of the consent model and the categorization of the consent managers as NBFCs. The PSD2 in the European Union, which facilitated the growth of fintech in the region, resulted in a fragmented API marketplace and a mere 5% penetration in the European market, prompting the need to develop PSD3. The AUD 1.5 billion Consumer Data Right in Australia, which achieved a mere 1% penetration and a much-needed strategic reset recognized by the government, is in need of a revival. The paper finds that India's AA model offers structural advantages in consent granularity, privacy-by-design, and adoption velocity, while lagging in mandatory participation and consumer redress, and concludes that its design philosophy offers transferable lessons for open finance governance in emerging economies.

Index Terms - **Account Aggregator, Open Banking, PSD2, Consumer Data Right, Open Finance Regulation, Consent Architecture, Digital Public Infrastructure, Financial Data Sharing, Comparative Regulation, India, European Union, Australia.**

Glossary:
Account Aggregator (AA): A licensed Non-Banking Financial Company in India that acts as a consent-based data intermediary, routing encrypted financial data between Financial Information Providers and Financial Information Users without storing or accessing the data itself.
ACCC (Australian Competition and Consumer Commission): The primary regulatory authority overseeing Australia's Consumer Data Right, responsible for accreditation of data recipients and enforcement of CDR Rules.

API (Application Programming Interface): A set of technical protocols that allows different software systems to communicate with each other. In open banking, APIs enable banks and financial institutions to securely share customer data with authorised third parties.

Consent Artefact: A digitally signed, machine-readable record within India's AA framework that specifies the terms of a customer's data sharing authorisation - including who receives the data, what data is shared, for what purpose, for how long, and at what frequency. Can be revoked by the customer at any time.

Consumer Data Right (CDR): Australia's legislative framework granting consumers the right to direct their financial, energy, and telecommunications data to accredited third parties. Governed by the ACCC, OAIC, and Data Standards Body.

Data Standards Body (DSB): An Australian government body within Treasury responsible for setting binding technical API standards for the Consumer Data Right framework.

DEPA (Data Empowerment and Protection Architecture): A policy framework developed by NITI Aayog, Government of India, articulating the philosophical and technical principles underpinning India's consent-based data sharing ecosystem, including the Account Aggregator framework.

Digital Public Infrastructure (DPI): Shared digital systems built on open standards that function as foundational national infrastructure. India's DPI stack includes Aadhaar (identity), UPI (payments), and the Account Aggregator framework (data sharing).

FIU (Financial Information User): Any regulated financial entity - lender, wealth manager, fintech platform - that requests access to a customer's financial data through the AA framework for a specified purpose.

FIP (Financial Information Provider): Any entity that holds a customer's financial data - banks, NBFCs, insurance companies, mutual fund houses, pension funds, GSTN - and is authorised to share it through the AA framework upon receipt of a valid consent artefact.

FIDA (Financial Data Access Regulation): A proposed EU regulation that would extend open finance obligations beyond payment accounts to investments, insurance, and pensions - effectively expanding PSD2's scope to cover the full financial data landscape.

GSTN (Goods and Services Tax Network): India's government-managed IT infrastructure for GST administration. Its inclusion as an FIP in the AA framework in 2025 enables lenders to access GST return data for MSME credit assessment.

NBFC (Non-Banking Financial Company): A company registered under the Companies Act and regulated by the RBI that provides financial services but does not hold a banking licence. Account Aggregators are currently classified as a category of NBFC.

OAIC (Office of the Australian Information Commissioner): Australia's independent privacy regulator, responsible for overseeing privacy compliance within the Consumer Data Right framework.

Open Banking: A regulatory model requiring banks to share customer financial data with authorised third parties through secure APIs, upon customer consent, to promote competition and innovation in financial services.

Open Finance: An extension of open banking principles beyond payment accounts to the full spectrum of financial products - investments, insurance, pensions, lending - enabling comprehensive consumer financial data portability.

PSD2 (Second Payment Services Directive): European Union Directive 2015/2366, which mandated that banks provide licensed third-party providers with API access to customer payment account data upon consent, establishing the EU's open banking regime from January 2018.

PSD3 (Third Payment Services Directive): The proposed successor to PSD2, introduced by the European Commission in June 2023, addressing PSD2's limitations in fraud prevention, API standardisation, and open banking adoption, with implementation anticipated from 2026-2027.

PSR (Payment Services Regulation): A directly applicable EU regulation proposed alongside PSD3, which would replace certain PSD2 provisions with uniform rules across all member states, eliminating the inconsistencies produced by national transposition of PSD2.

RBI (Reserve Bank of India): India's central bank and the primary regulator of the Account Aggregator framework, responsible for licensing AAs as NBFCs and supervising their operations.

SCA (Strong Customer Authentication): A PSD2 requirement mandating two-factor authentication - combining something the user knows, has, and is - for most electronic payment transactions, to reduce fraud.

Screen Scraping: An older, less secure method of financial data sharing in which a third party accesses a customer's bank account by using the customer's login credentials to extract data directly from the bank's website. Being phased out in favour of secure API-based data sharing across all three jurisdictions studied.

TPP (Third Party Provider): Under PSD2, a licensed entity authorised to access customer payment account data. Includes Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs).

UPI (Unified Payments Interface): India's real-time payment system, developed by the National Payments Corporation of India, enabling instant fund transfers across bank accounts through a mobile platform. Recognised as a foundational layer of India's Digital Public Infrastructure.

XS2A (Access to Account): The core mechanism of PSD2 requiring banks to provide licensed TPPs with access to customer payment accounts through secure APIs upon customer consent.

1. Introduction

The digitization of financial services has made consumer financial data the focus of a new set of rules. As financial institutions, fintech firms, and technology platforms gain a competitive edge from access to detailed transactional and behavioral data, regulators in different countries have had to answer a basic question: who owns financial data and under what conditions can it be shared? The policy responses to this question have led to the creation of a new type of regulation known as open banking, open finance, or data empowerment architecture. This type of regulation aims to protect consumers' rights to their financial data while also allowing it to be shared safely between institutions.

Three jurisdictions have become the main points of reference for this type of regulation. The European Union's PSD2 law set up the first large-scale mandatory open banking system. It granted third parties the right to access payment account data. Next came the Consumer Data Right in Australia. This is the most ambitious open data framework in the world in terms of sectoral scope, extending consumer data portability rights across banking, energy, and telecommunications. India, through its Account Aggregator framework, pursued a structurally different path: rather than mandating data access as a competition remedy, it built a dedicated consent management infrastructure - the Account Aggregator - as a licensed intermediary sitting between data holders and data users, routing encrypted financial data flows without itself accessing the underlying data.

By early 2026, the divergence in outcomes across these three frameworks is both striking and analytically significant. The Account Aggregator (AA) framework in India has expanded its user base to 252.9 million users and 2.61 billion enabled accounts. The framework has enabled total loan disbursements of ₹1.3 lakh crore since September 2021. The Indian Union Budget recognizes the Account Aggregator framework as a vital component of Digital Public Infrastructure, as are Aadhaar and the Unified Payments Interface (Department of Financial Services, 2025; Invest India, 2023). The Payment Services Directive 2 (PSD2) in the European Union, though a catalyst for the development of fintech in the region, saw the API landscape and consumer adoption rate fragment below 5 percent, prompting the European Commission to propose the PSD3 and Financial Data Access regulations (European Commission, 2023). The Consumer Data Rights (CDR) in Australia, which saw industry incur AUD 1.5 billion in compliance costs since 2018 while gaining a consumer adoption rate below 1 percent, is officially recognized as undergoing a strategic reset in 2025-2026, with the government acknowledging the phenomenon as a result of a "good idea, badly executed" (Accenture, 2024; Lexology, 2026).

These divergent trajectories invite a comparative regulatory analysis that goes beyond surface-level description. While the growing literature on open banking regulation has extensively examined PSD2 and, to a lesser extent, the CDR, India's AA framework remains systematically underrepresented in comparative scholarship. Studies that do reference the AA tend to treat it as a peripheral case note rather than as a primary subject of regulatory design analysis. This gap is consequential: as open finance regulation expands across Asia, Africa, and Latin America, the design choices embedded in the AA framework - particularly its consent intermediation model, privacy-by-design architecture, and open technical standards - warrant structured examination alongside the established Western frameworks.

This paper addresses that gap through a structured comparative analysis of the AA framework, PSD2, and CDR along five regulatory design parameters: consent architecture, mandatory participation, liability allocation, interoperability standards, and enforcement mechanisms. The analysis draws on regulatory instruments, institutional reports, and industry data across all three jurisdictions. The paper does not seek to rank these frameworks in absolute terms, but to identify the specific design choices that have produced observed outcomes, and to derive implications for the evolution of open finance governance in India and comparable emerging economies.

The remainder of the paper is structured as follows. Section II presents the literature review. Section III analyses India's AA framework. Section IV examines PSD2 and CDR. Section V presents the comparative analysis. Section VI outlines the results, implications, and avenues for further research.

2. Literature review

The comparative study of open finance regulation has grown substantially since the mid-2010s, though India's Account Aggregator framework remains underrepresented in this body of work.

The Basel Committee on Banking Supervision (2019) provides the foundational cross-jurisdictional taxonomy for open banking regulation, classifying approaches across 25 member jurisdictions into prescriptive, facilitative, and market-driven models, placing both the EU and India within the prescriptive category. This paper argues, however, that this classification obscures fundamental differences in how each jurisdiction has operationalised its framework in practice - particularly in consent architecture, intermediary design, and liability allocation.

India's AA framework originates in the RBI's Master Directions of 2016 and was officially launched on September 2, 2021, establishing Account Aggregators as NBFCs functioning as consent-based data intermediaries between Financial Information Providers and Financial Information Users (Reserve Bank of India via PIB, 2021). NITI Aayog's Data Empowerment and Protection Architecture (DEPA, 2020) articulates the philosophical foundation of this model, contrasting it with Western open banking approaches by segregating consent collection from data provision. Raghavan and Singh (2020), in the most rigorous academic treatment of the AA's regulatory design, critically examine the RBI's classification of AAs as NBFCs, arguing

that this regulatory form is structurally misaligned with the AA's actual function as a data flow intermediary rather than a financial services provider - a tension that remains unresolved in the current framework. Invest India (2023) positions the AA as India's third Digital Public Infrastructure, while the Department of Financial Services (2025) confirms 126 institutions live as both FIP and FIU and over 2.61 billion accounts enabled. According to the CGAP report (2025), the growth has been restricted to business-to-business lending transactions, with consumer retail uptake significantly lagging. This has been reinforced by a report from the Economic Times (2025), wherein the SBI Managing Director, Ashwini Kumar Tewari, pointed out that the single consent mechanism was a structural trust and privacy risk and has cautioned the industry that regulatory action may be required if the industry fails to correct this internally.

The EU's PSD2 (Directive 2015/2366, 2018) has mandated access to payment account data through the access to account rule but has been technology-neutral, leaving the standardization of APIs to individual banks. The European Commission's own evaluation (VVA/CEPS, 2022) reported that less than 5% of EU consumers were active users of open banking by 2021, which it attributed to the fragmented nature of API standards. The draft for PSD3 and the proposed Financial Data Access Regulation indicate the institution's recognition of the failure of the market-led approach to technical standards adopted for PSD2.

Australia's Consumer Data Right (CDR), introduced via the Treasury Laws Amendment (Consumer Data Right) Bill 2019, is based on a rights-based paradigm supported by mandatory technical standards set by the Data Standards Body, with the Australian Competition and Consumer Commission (ACCC) maintaining oversight. Nevertheless, as revealed by the Accenture CDR Strategic Review (2024), even though the architecture appears robust, only 0.31% of bank customers were actively using CDR by the end of 2023, with the industry incurring AUD 1.5 billion in compliance-related costs since 2018. The Australian government has set a new strategic course for the CDR, focusing on high-value use cases, reducing compliance for smaller participants, and implementing a comprehensive prohibition on screen scraping to drive the industry towards the CDR framework (Lexology, 2026; Mastercard, 2026).

There is still no structured comparative analysis of the AA, PSD2, and CDR that uses the same regulatory design parameters in the available literature. This paper addresses that gap directly.

3. India's account aggregator framework

3.1 Regulatory Foundation And Design Philosophy

India's Account Aggregator architecture was conceptualized by the RBI in July 2015 and formally introduced via the Master Direction – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions, 2016. The Account Aggregator architecture was formally operationalized on 2nd September 2021, as eight major banks simultaneously commenced live operations as Financial Information Providers (Reserve Bank of India via PIB, 2021). The RBI's foundational design choice - classifying AAs as a new category of NBFC rather than as a standalone data intermediary - has significant regulatory implications. Raghavan and Singh (2020) argue that this classification is structurally misaligned with the AA's actual function: unlike conventional NBFCs which provide financial services, AAs neither lend, invest, nor hold customer funds. They operate exclusively as encrypted data conduits, blind to the content of the information they carry. The NBFC classification subjects AAs to capital adequacy requirements, RBI licensing conditions, and supervisory frameworks designed for financial services providers - a regulatory overhead that arguably reflects an imperfect fit between the entity's function and its legal form.

The conceptual architecture underpinning the framework is NITI Aayog's Data Empowerment and Protection Architecture (DEPA, 2020), which articulates a deliberate departure from Western open banking models. Where PSD2 and CDR enable third parties to access data held by banks, DEPA's consent manager model interposes a dedicated intermediary whose sole function is consent management - separating the act of consent from both the data holder and the data user. This segregation, NITI Aayog argues, provides stronger structural privacy guarantees than models where data providers manage consent directly alongside their commercial relationships with customers.

3.2 Architecture: The Three-Party Model

The AA framework operates through three distinct participant categories. Financial Information Providers (FIPs) are entities that hold customer financial data - banks, NBFCs, insurance companies, mutual fund houses, pension funds, and, as of 2025, the Goods and Services Tax Network (GSTN), whose inclusion as an FIP significantly expands the framework's utility for MSME credit assessment (Department of Financial Services, 2025). Financial Information Users (FIUs) are regulated financial entities that request access to customer data - typically lenders, wealth managers, and fintech platforms. The Account Aggregator sits between them, managing the consent artefact - a digitally signed, machine-readable record of the customer's data sharing authorisation - and routing encrypted data flows from FIP to FIU without retaining or accessing the data itself.

This zero-storage, blind-conduit architecture is the framework's most distinctive technical feature. The AA cannot read, store, or monetise the data it carries. Every data transfer is tied to a specific, time-bound, purpose-limited consent artefact that the customer can revoke at any time. This design directly addresses the data misuse risks that have attracted regulatory scrutiny in other jurisdictions - most notably the screen scraping practices that predated open banking APIs in the EU and Australia, and which Australia is now formally moving to ban (Mastercard, 2026).

3.3 Ecosystem Scale and Lending Outcomes

By early 2026, the AA ecosystem has achieved substantial scale. The Department of Financial Services (2025) reports 126 financial institutions live as both FIP and FIU, 50 live as FIP only, and 754 as FIU only, across banking, insurance, and pension sectors. Over 2.61 billion financial accounts are enabled for data sharing, with 252.9 million users having linked their accounts. The Sahamati H1 FY25 report (Economic Times, March 2025) documents ₹74,500 crore disbursed through the AA framework in the first half of FY2025 alone, with total disbursements of ₹1.3 lakh crore since inception across 9.70 million loans. NBFCs account for over 65 percent of total consents, with private sector banks contributing over 9 percent. Personal loan penetration through the AA has reached 10.52 percent, with MSME lending penetration at 1.14 percent - modest but growing. The framework's recognition in India's Union Budget as a pillar of Digital Public Infrastructure, alongside Aadhaar and UPI, signals its elevation from a sectoral regulatory instrument to a national economic infrastructure (Invest India, 2023).

3.4 Challenges and Structural Tensions

Despite its scale, the AA framework faces three categories of challenge. First, the retail adoption gap: CGAP (2025) documents that growth remains concentrated in B2B lending transactions, with a 10-percentage-point awareness gap between male and female users, and significantly lower usage among less educated segments. Second, the consent quality problem: SBI Managing Director Ashwini Kumar Tewari, speaking at IFTA 2025, publicly flagged that the single consent mechanism - applied uniformly across loans, wealth management, and account openings - means most customers authorise data sharing without understanding the scope of what they have permitted (Economic Times, December 2025). Tewari makes a direct analogy with the General Data Protection Regulation (GDPR) and suggests that the Indian consent-based architecture does not meet the requirement for informed and specific consent as a requirement of data protection regulations, and that regulatory intervention, including prohibition, remains a threat if the industry does not self-correct. The structural tension relating to the NBFC status also remains unresolved, as revealed by Raghavan and Singh (2020), who note that the regulatory form for the Account Aggregator architecture was intended for financial services providers, not data operators, and the implications for the supervision, capitalization, and accountability of Account Aggregators remain.

4. The Eu's Psd2 And Australia's Consumer Data Right

4.1 The European Union's Psd2

The European Union's Second Payment Services Directive (Directive 2015/2366, also called PSD2), which entered into force in the EU's member states as of January 2018, is the first mandatory open banking regime on a global scale. The XS2A requirement, the core innovation of the directive, obligated banks to allow API-based access to the data contained in customers' payment accounts to TPPs that have been authorized by the relevant national regulatory authority. The TPPs are divided into two categories: Account Information Service Providers (AISPs), whose services allow users to aggregate information from multiple accounts, and Payment Initiation Service Providers (PISPs), who allow users to make direct payments from their accounts. The latter have to register with the national competent authority, and Strong Customer Authentication, consisting of a two-factor authentication requirement, is mandatory for the majority of electronic payment transactions.

PSD2's foundational regulatory rationale was competition rather than consumer empowerment. The aim of the directive was to break the structural data power held by incumbent banks by compelling data sharing with authorized third parties, thus lowering the barriers for new entrants in the fintech industry and stimulating innovation in the payment services industry as a whole. This competition rationale distinguished PSD2 from both DEPA's individual empowerment philosophy and CDR's rights-based architecture - a distinction with significant consequences for how each framework was designed and what outcomes it produced.

PSD2's most consequential structural choice was technology neutrality. PSD2 required access without dictating a single API standard. Instead, the technical implementation of the API was left to the individual banks. As a result, the open banking ecosystem became fragmented. By 2021, the quality, reliability, and level of documentation of the API offered by banks across the EU varied significantly. This created asymmetric market conditions for TPPs to develop services across the EU. The European Commission's own evaluation (VVA/CEPS, 2022) found that fewer than 5 percent of EU consumers were active open banking users by 2021 - a figure that starkly illustrated the gap between the directive's competition objectives and its market outcomes. The evaluation attributed this shortfall to inconsistent national transposition, uneven API quality, and the absence of a mandated technical standard.

The EU's response has been to propose a successor framework. In June 2023, the European Commission published a draft of PSD3, along with a proposed Payment Services Regulation (PSR). The proposed regulation will extend the open finance regime to cover not just payments but also investments, insurance, and pensions through the proposed Financial Data Access (FIDA) regulation. The implementation of PSD3 is expected to commence circa 2026-2027. The proposals introduce IBAN name verification to combat spoofing fraud, stronger performance requirements for bank APIs, and non-bank payment service providers' direct access to EU payment systems - each addressing a specific failure mode of PSD2 (ACI Worldwide, 2026; European Commission, 2023). The transition from PSD2 to PSD3 is analytically significant for this paper: it represents the EU's institutional acknowledgment that a market-driven, technology-neutral approach to open banking standardisation was insufficient, and that more prescriptive infrastructure intervention is required - a conclusion that India's AA framework reached by design in 2016.

4.2 Australia's Consumer Data Right

Australia's Consumer Data Right, introduced through the Treasury Laws Amendment (Consumer Data Right) Bill 2019, is the most ambitious open data regime in terms of sectoral coverage. Unlike PSD2, which relies on a competitive analysis for the open banking regime, the CDR takes a rights-based approach to open data. It treats data portability as a consumer right, allowing consumers to direct their data to third-party organizations. The Australian Competition and Consumer Commission (ACCC) serves as the primary regulatory authority for accreditation and rules, while the Office of the Australian Information Commissioner (OAIC) oversees privacy compliance, and the Data Standards Body (DSB) within Treasury sets binding technical API standards - a degree of prescriptive standardisation deliberately absent from PSD2.

Despite this architectural rigour, CDR's empirical record through its first five years has been deeply disappointing. The Accenture CDR Strategic Review (2024), commissioned by the Australian Banking Association, found that as of end-2023, only 0.31 percent of bank customers had an active CDR data sharing arrangement, with the banking industry having invested approximately AUD 1.5 billion in compliance costs since 2018. The review attributed this failure to an absence of compelling consumer value propositions, excessive compliance complexity particularly for mid-tier and smaller institutions, and a governance framework that prioritised regulatory completeness over user experience. The review notably observed that market-supported open data models in India and Singapore achieved significantly higher adoption rates - a direct comparative point of relevance to this paper's analysis.

By early 2026, the Australian government has acknowledged these failures and initiated what it formally describes as a strategic reset. The government's characterisation of CDR as a "good idea, badly executed" is not rhetorical: it has prompted concrete legislative and regulatory action (Lexology, 2026). Action initiation legislation has passed, enabling write access - meaning accredited third parties will soon be able to initiate actions such as switching bank accounts or energy providers, rather than merely reading data (Mastercard, 2026). Treasury has been formally tasked with planning a full ban on screen scraping, compelling financial institutions toward CDR-compliant API-based data sharing. New API standards, including version 5 for Product Details, are being phased in as of March 2026, with older versions retired. Digital ID alignment efforts are underway to integrate CDR with Australia's new Digital ID laws, reducing friction in the consumer consent process (Lexology, 2026). For non-bank lenders, mandatory data sharing obligations for large providers commence in mid-July 2026, with full rollout across all non-bank lenders concluding around mid-September 2027.

The CDR's strategic reset trajectory is analytically significant in two respects. First, it confirms that prescriptive mandatory frameworks with high compliance costs and insufficient consumer value propositions produce adoption failure regardless of their technical sophistication. Second, the reset's specific remediation measures - simplified consent, write access, screen scraping ban, digital identity integration - converge toward design features that India's AA framework incorporated at inception. This convergence is noted in the comparative analysis that follows.

5. Comparative Analysis

This section applies the five regulatory design parameters - consent architecture, mandatory participation, liability allocation, interoperability standards, and enforcement mechanisms - across the three frameworks. The analysis draws on the preceding sections to identify the specific design choices that have produced observed outcomes, and to derive implications for open finance governance.

5.1 Consent Architecture

Consent architecture is the parameter on which the three frameworks diverge most fundamentally, and where the consequences of divergence are most visible in adoption and trust outcomes.

India's AA framework builds consent into the infrastructure layer through the consent artefact - a digitally signed, machine-readable record specifying the data requester, data type, purpose, frequency, and duration of sharing. The consent artefact is generated, stored, and managed by the AA, which acts as a neutral intermediary with no commercial interest in the data transaction. Customers can view, modify, and revoke consents at any time through the AA interface. NITI Aayog's DEPA (2020) argues that this structural separation of consent management from both data holding and data use provides stronger privacy guarantees than models where commercial entities manage consent alongside their service relationships. However, Tewari's critique (Economic Times, 2025) exposes a practical vulnerability: the single consent mechanism, applied uniformly across all financial services products, has in practice produced blanket authorisations that customers do not fully understand - undermining the informed, specific consent that the architecture theoretically guarantees. This gap between architectural intent and behavioural reality is the AA framework's most pressing consent design challenge.

PSD2's consent model is comparatively thin. The directive requires customer consent for TPP data access but prescribes no specific consent architecture, leaving consent design to individual TPPs and banks. SCA provides authentication rigour for payment transactions but does not address the quality or granularity of data sharing consent. The result is that consent under PSD2 is often embedded within TPP terms and conditions, lacking the specificity, revocability, and transparency that the AA's consent artefact provides by design. The proposed FIDA regulation acknowledges this gap by introducing financial data access dashboards - tools that would allow consumers to view and manage data sharing permissions - converging toward the consent visibility that India's AA has offered since inception.

Australia's CDR consent model is the most prescriptive of the three. The CDR Rules specify detailed consent requirements including purpose limitation, expiry, and consumer-facing dashboards for consent management. The OAIC's involvement ensures privacy law alignment. However, the complexity of the consent process has been identified as a primary adoption barrier: the Accenture review (2024) found that consumer consent flows were perceived as burdensome and confusing, contributing directly to the framework's sub-1 percent adoption rate. The strategic reset's emphasis on simplification acknowledges that prescriptive consent design, while legally rigorous, can be counterproductive if it produces friction that deters consumer participation.

5.2 Mandatory Participation

The degree to which data holders are compelled to participate in the open finance ecosystem is a critical determinant of ecosystem completeness and, by extension, the value proposition available to consumers and FIUs.

PSD2's mandatory participation obligation is narrow but binding: banks must provide API access to licensed TPPs for payment account data. However, the directive does not extend mandatory participation to non-payment financial data - investments, insurance, pensions - leaving these categories to the proposed FIDA regulation. Within its scope, PSD2's mandatory access rule has been effective in compelling bank API provision, though quality and reliability have varied significantly across institutions.

Australia's CDR imposes the most comprehensive mandatory participation obligations of the three frameworks. The staged rollout - beginning with the Big Four banks, expanding to all banks, and now extending to non-bank lenders from mid-2026 and energy providers - ensures systematic ecosystem expansion. The DSB's binding technical standards apply uniformly to all participants, eliminating the API fragmentation that undermined PSD2. However, the compliance cost of mandatory participation has been disproportionately burdensome for smaller institutions, a structural inequity that the strategic reset is specifically attempting to address through cost reduction measures for smaller participants (Lexology, 2026).

India's AA framework has no mandatory participation obligation for FIPs. Financial institutions join the ecosystem voluntarily, and while 126 institutions are live as of early 2026, participation remains uneven across sectors. Insurance and pension FIPs are significantly underrepresented relative to banking FIPs, limiting the AA's utility for comprehensive financial profiling. The absence of a mandatory participation requirement means that the ecosystem's completeness is dependent on commercial incentives rather than regulatory compulsion - a structural vulnerability that becomes particularly acute in the context of MSME credit assessment, where the value of AA-enabled underwriting depends on the breadth of data accessible through the framework. The GSTN's addition as an FIP in 2025 partially addresses this gap for MSME use cases, but the broader participation deficit remains an unresolved policy question.

5.3 Liability Allocation

Liability allocation - determining which party bears responsibility when data is shared without proper consent, used beyond its authorised purpose, or involved in a fraud event - is a parameter on which all three frameworks exhibit significant gaps, though in different ways.

PSD2 establishes relatively clear liability rules within its payment services scope: banks are liable for unauthorised payment transactions unless they can demonstrate customer fraud or gross negligence, and TPPs bear liability for losses attributable to their unauthorised or erroneous access. However, these liability rules apply specifically to payment transactions and do not extend cleanly to account information services, where the consequences of data misuse are less immediately quantifiable than a fraudulent payment.

CDR's liability framework is more elaborate, establishing a tiered accreditation system - unrestricted, restricted, and sponsored accreditation - with liability obligations calibrated to accreditation tier. The OAIC's oversight ensures alignment with the Privacy Act, providing consumers with regulatory recourse for data misuse. However, the complexity of the accreditation and liability framework has contributed to the compliance cost burden that has deterred smaller participants.

India's AA framework's liability architecture is its least developed dimension. The RBI Master Directions establish the AA's obligations as a licensed NBFC but do not comprehensively address liability allocation between FIPs, FIUs, and AAs in the event of data breach, consent violation, or misuse. Raghavan and Singh (2020) identify this as a significant regulatory gap, noting that the absence of clear liability rules creates uncertainty for all ecosystem participants and may deter institutional participation. The NBFC classification of AAs adds a further complication: NBFC regulatory frameworks were not designed with data intermediary liability in mind, and the resulting regulatory ambiguity is a structural consequence of the classification choice the RBI made in 2016.

5.4 Interoperability Standards

Interoperability - the ability of different participants' technical systems to communicate seamlessly - is the parameter most directly linked to ecosystem fragmentation risk, and the one on which the three frameworks have made the most divergent choices.

India's AA framework achieves interoperability through the DEPA technical standards, developed by Sahamati and mandated for all ecosystem participants. The standards specify API design, data formats, consent artefact structure, and encryption requirements, ensuring that any FIP can communicate with any AA and any FIU without bilateral technical negotiation. This standardisation at the infrastructure layer is the AA's most significant structural advantage over PSD2, and it is the design feature that Australia's CDR most closely replicates through the DSB's binding technical standards. The practical consequence is visible in the AA's consent transaction growth rate of 12 percent per month (Economic Times, March 2025) - a figure that reflects the frictionless technical interoperability the standards enable.

PSD2's technology-neutral approach produced the opposite outcome. Without a mandated common standard, bank APIs across the EU diverged in design, documentation quality, and reliability. The European Banking Authority's regulatory technical standards provided some harmonisation for SCA but did not extend to API design for account information services. The result was an ecosystem where TPPs faced significant technical overhead in integrating with multiple banks across member states - a structural friction that directly contributed to PSD2's adoption shortfall and is a primary driver of the PSD3 reform agenda.

Australia's DSB standards represent the most technically prescriptive approach of the three frameworks, specifying detailed API requirements that are regularly updated - with version 5 for Product Details being phased in as of March 2026. This prescriptiveness has delivered interoperability within the CDR ecosystem but has also contributed to compliance costs, as institutions must continuously update their technical

implementations to meet evolving standards. The balance between standardisation rigour and compliance burden is a design tension that all three frameworks navigate differently, with India's AA currently achieving the most favourable equilibrium.

5.5 Enforcement Mechanisms

Enforcement - the regulatory apparatus available to compel compliance, investigate violations, and sanction misconduct - is the parameter on which India's AA framework is most clearly underdeveloped relative to its peers.

PSD2's enforcement is distributed across national competent authorities in each EU member state, with the European Banking Authority providing coordination and guidance. Sanctions for non-compliance vary by jurisdiction, but the directive's mandatory access rule gives TPPs legal standing to challenge bank non-compliance - a mechanism that has been used in several jurisdictions to compel API provision. The transition to PSD3 will introduce a Payment Services Regulation directly applicable across all member states without national transposition, strengthening enforcement consistency.

CDR's enforcement architecture is the most comprehensive of the three frameworks. The ACCC holds accreditation and rules enforcement powers, the OAIC holds privacy enforcement powers, and the DSB holds technical standards authority. This tripartite structure, while potentially complex, provides overlapping enforcement coverage across commercial, privacy, and technical dimensions. Consumer redress mechanisms are embedded in the CDR Rules, providing individuals with regulatory recourse for data misuse - a feature absent from India's AA framework.

India's AA framework relies primarily on RBI supervisory oversight of licensed AAs as NBFCs. The RBI's enforcement powers are substantial in the context of NBFC supervision, but the AA's regulatory form as an NBFC means that enforcement is oriented toward financial services conduct rather than data intermediary conduct. There is no dedicated enforcement mechanism for consent violations, no consumer redress framework for data misuse through the AA channel, and no regulatory standing for FIUs or customers to challenge FIP non-participation. Tewari's warning (Economic Times, 2025) that regulatory intervention - potentially including a ban - remains possible if consent mechanism design is not improved reflects the enforcement vacuum: absent proactive industry self-regulation, the RBI's primary enforcement lever is the blunt instrument of restriction or prohibition rather than graduated, conduct-specific sanction.

5.6 Comparative Summary

The following table summarises the comparative assessment across all five parameters:

Parameters	Indian AA	EU's PSD2	Australian CDR
Consent Architecture	Strong by design, weakened in practice by single consent mechanism	Thin, with no explicit prescriptive framework	Prescriptive in nature, but heavy in user friction
Mandatory Participation	Voluntary, with ecosystem gaps persisting	Mandatory, only for payment accounts	Mandatory, with sector-by-sector rollout
Liability Allocation	Underdeveloped, with notable gaps	Clearly defined for payments, with gaps persisting for data services	Accreditation model, with tiered structure; most developed of the three
Interoperability Standards	Strong, with mandated open standards	Weak, with technology-neutral approach failing to drive robust interoperability	Strong, with standards mandated by Data Standards Board (DSB)
Enforcement Mechanisms	Underdeveloped, with supervisory model aligned to NBFCs	Distributed model, with enhancements ongoing as part of PSD3	Comprehensive model, with tripartite framework

The comparative picture that emerges is one of complementary strengths and weaknesses. India's AA framework leads on consent architecture design and interoperability standardisation, and its adoption trajectory significantly outperforms both PSD2 and CDR in consumer and transaction volume terms. However, it lags materially on mandatory participation, liability allocation, and enforcement - the three parameters most critical to long-term ecosystem trust and institutional accountability. PSD2's competition-driven rationale produced API access at scale but without the consent quality or technical standardisation necessary for meaningful consumer engagement. CDR's rights-based, prescriptive approach achieved the most legally rigorous framework design but at a compliance cost that has suppressed adoption and necessitated a fundamental strategic reset. The convergence of PSD3 and CDR's reset agenda toward design features the AA incorporated at inception - standardised APIs, consent dashboards, screen scraping prohibition - suggests that the AA's foundational architecture is being retrospectively validated by the remediation choices of more established frameworks.

6. Conclusion And Policy Recommendations

6.1 Summary of Findings

This paper set out to examine how three jurisdictions - India, the European Union, and Australia - have operationalised the shared goal of consumer-controlled financial data sharing, and with what regulatory design consequences. The comparative analysis across five parameters yields three principal findings.

First, architectural philosophy determines adoption trajectory more than regulatory compulsion. India's AA framework, built on a privacy-by-design consent intermediation model with mandated open technical standards, has achieved adoption velocity that materially outpaces both PSD2 and CDR despite the absence of mandatory FIP participation. The EU's technology-neutral approach and Australia's compliance-heavy prescriptive model both produced adoption failures that are now being remediated through design changes that converge toward features the AA incorporated at inception. This convergence constitutes a form of retrospective validation of India's foundational design choices.

Second, scale is not sufficient evidence of framework maturity. The AA's impressive headline figures - 252.9 million users, 2.61 billion enabled accounts, ₹1.3 lakh crore in cumulative disbursements - obscure structural vulnerabilities that, if unaddressed, risk undermining the framework's long-term credibility. The retail adoption gap documented by CGAP (2025), the consent quality problem flagged by Tewari (Economic Times, 2025), the liability allocation gaps identified by Raghavan and Singh (2020), and the absence of a consumer redress framework collectively represent a regulatory debt that the framework's growth metrics do not yet reflect.

Third, the NBFC classification of Account Aggregators remains the framework's most consequential unresolved structural question. As Raghavan and Singh (2020) argue, the regulatory form governing AAs was designed for financial services providers, not for neutral data infrastructure operators. The mismatch has downstream consequences for supervision, liability, enforcement, and the regulatory imagination of what an AA can and cannot do. As the framework matures and its role in India's financial infrastructure deepens, the appropriateness of the NBFC classification warrants formal regulatory reconsideration.

6.2 Policy Recommendations

Drawing on the comparative analysis, this paper proposes four specific policy recommendations for the evolution of India's AA framework.

Mandatory FIP Participation for Systemically Important Institutions: The voluntary participation model has produced uneven ecosystem coverage, particularly in insurance and pension data. The RBI should introduce mandatory FIP participation obligations for systemically important financial institutions - large banks, major insurance companies, and primary pension fund managers - while retaining voluntary participation for smaller

entities. This targeted mandate would materially improve ecosystem completeness without imposing the compliance cost burden that has undermined CDR's smaller participant engagement.

Consent Architecture Reform: The single consent mechanism must be replaced with a purpose-specific, granular consent model that requires separate, informed authorisation for each distinct use case - credit underwriting, wealth management, account opening - rather than a single blanket authorisation. This reform directly addresses Tewari's concern (Economic Times, 2025) and aligns the AA's consent practice with the architectural intent of the DEPA framework. The reform should be accompanied by mandatory plain-language consent disclosures, drawing on Australia's CDR consumer dashboard experience as a design reference.

Dedicated Liability and Consumer Redress Framework: The RBI should issue supplementary directions establishing clear liability allocation between FIPs, AAs, and FIUs for data breaches, consent violations, and data misuse, alongside a consumer redress mechanism providing individuals with regulatory recourse independent of the NBFC supervisory channel. CDR's tripartite enforcement structure - separating commercial, privacy, and technical enforcement - offers a useful reference model, adapted to India's regulatory architecture.

Regulatory Reclassification of Account Aggregators: The RBI should initiate a formal review of the NBFC classification of AAs, with a view to creating a dedicated regulatory category - a Consent Manager or Data Intermediary licence - that is purpose-designed for entities whose sole function is consent-based data intermediation. This reclassification would align the regulatory form with the entity's function, enable supervision frameworks appropriate to data infrastructure operators, and resolve the liability and enforcement ambiguities that the current NBFC classification produces.

6.3 Broader Implications

Beyond India, the comparative analysis of this paper carries implications for open finance governance in emerging economies more broadly. The AA framework's foundational design - separating consent management from data provision, building on open technical standards, and embedding privacy protection at the infrastructure layer rather than as a regulatory overlay - offers a replicable architecture for jurisdictions seeking to develop open finance ecosystems without the compliance costs and adoption failures that have characterised the EU and Australian experiences. The recognition of the AA as Digital Public Infrastructure, alongside Aadhaar and UPI, during India's G20 Presidency signals a growing international interest in the Indian model as a template for data-driven financial inclusion. The policy recommendations advanced in this paper are intended to strengthen that template by addressing its current structural gaps before they become systemic risks.

6.4 Limitations and Future Research

This paper is limited by its reliance on secondary sources and its inability to incorporate primary empirical data on consumer consent behaviour, institutional participation incentives, or regulatory enforcement outcomes within the AA ecosystem. Future research should examine the behavioural dimensions of consent quality - specifically whether granular consent architectures produce meaningfully better-informed authorisation decisions or merely impose additional friction - and should assess the AA framework's performance specifically in MSME credit access, where the integration of GSTN as an FIP creates new empirical conditions for study. A longitudinal comparison of adoption trajectories across the three frameworks, as PSD3 and CDR's strategic reset produce new outcome data through 2026 and 2027, would further enrich the comparative literature this paper contributes to.

7. References

1. Accenture. 2024. CDR Strategic Review. Australian Banking Association, ausbanking.org.au

2. ACI Worldwide. 2026. PSD2 to PSD3: Key Updates and Current Landscape. aciworldwide.com

3. Australian Competition and Consumer Commission. 2024. Consumer Data Right Rules and Standards. accc.gov.au

4. Basel Committee on Banking Supervision. 2019. Report on Open Banking and Application Programming Interfaces. Bank for International Settlements, bis.org

5. Consultative Group to Assist the Poor. 2025. Account Aggregator Ecosystem: Adoption and Access Gap Analysis. cgap.org

6. Department of Financial Services, Ministry of Finance, Government of India. 2025. Account Aggregator Framework: Dashboard and Progress Update. financialservices.gov.in

7. European Commission. 2023. Proposal for a Directive on Payment Services and Electronic Money Services (PSD3) and Payment Services Regulation (PSR). ec.europa.eu

8. European Commission, VVA Brussels and CEPS. 2022. Evaluation of Directive 2015/2366/EU on Payment Services in the Internal Market. ec.europa.eu

9. Invest India, Ministry of Commerce and Industry. 2023. Account Aggregator: India's Next Digital Public Infrastructure. investindia.gov.in

10. Kathuria, V. 2021. Data Empowerment and Protection Architecture: Concept and Assessment. Observer Research Foundation, orfonline.org

11. Lexology. 2026. Australia's CDR Strategic Reset: Key Developments 2025-2026. lexology.com

12. Mastercard. 2026. CDR Action Initiation and Screen Scraping Ban: Australia's Open Banking Update. mastercard.com

13. NITI Aayog, Government of India. 2020. Data Empowerment and Protection Architecture. niti.gov.in

14. Raghavan, M. and Singh, A. 2020. Regulation of Information Flows as Central Bank Functions? Implications from the Treatment of Account Aggregators by the Reserve Bank of India. Future of Finance Initiative, Dvara Research, dvara.com

15. Reserve Bank of India. 2016. Master Direction - Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions, 2016. rbi.org.in

16. Reserve Bank of India via Press Information Bureau. 2021. Launch of Account Aggregator Framework. pib.gov.in

17. Shukla, S. 2025. ₹74,500 crore disbursed via Account Aggregator in H1 FY25: Sahamati Report. Economic Times. economictimes.indiatimes.com

18. Treasury Laws Amendment (Consumer Data Right) Bill 2019. Parliament of Australia. legislation.gov.au

19. Tewari, A.K. via PTI. 2025. SBI MD flags concerns on Account Aggregator's single consent mechanism. Economic Times. economictimes.indiatimes.com