OpenID Foundation
2603 Camino Ramon, Suite 200
San Ramon, CA 94583

Honorable Ross Vought
Acting Director
Consumer Finance Protection Bureau
1700 G St NW
Washington, DC 20552

October 17, 2025

Acting Director Vought

Thank you for the opportunity to comment on CFPB-2025-0037, «Personal Financial Data Rights Reconsideration », which follows our prior submissions to the CFPB related to rule 1033 on December 29, 2023 and May 16 2024.

The OpenID Foundation (OIDF) is a non-profit, technical standards organization whose mission is to lead the global community in creating open, identity standards that are secure, interoperable and privacy-preserving. As part of that mission, we have worked closely with over 12 ecosystems to advance Open Banking and consumer financial data sharing globally. We hope to be of service to the CFPB as you refine this rule.

The OIDF's global community of private sector and public sector technical experts has developed the FAPI 2.0 security profile has become the global de-facto industry standard for API ecosystems in general, and especially widely adopted for Open Banking / Open Data ecosystems. OIDF's FAPI 2.0 Security Profile is itself a profile of the IETF's OAuth 2.0 and the OIDF's OpenID Connect. The FAPI profile is a security and interoperability enhanced version of OAuth 2.0 which closes critical security gaps that OAuth 2.0 alone does not address. The FAPI 2.0 profile has been selected by multiple leading private and public Open Banking ecosystems including those in Exhibit A to this letter.

In the countries that have adopted FAPI, we are seeing tangible adoption in the form of daily API calls by users and conformance to the standards:

- Billions of successful FAPI API calls, with secure, interoperable and consent-based

movement of user data or payments

- 55 million active users in Brazil (25% of the population)
- 15 million unique users in the UK (22% of adults/month), 2 Billion API calls per month (https://www.openbanking.org.uk/api-performance/)
- 3,500 FAPI implementations certified globally by OIDF (https://openid.net/certification/)

OIDF is a global leader in other standards deployed by the private and public sector alike. Beyond FAPI and open banking, OIDF specifications are widely recognized by government and public sector implementers including OpenID Connect (3+ billion users daily globally for login, single sing on), OpenID for Verifiable Presentation and Verifiable Credential Issuance (37 countries selected these OIDF specifications for digital wallets), and Shared Signals (recommended by US CISA). Our standards such as OpenID Connect have also been recognized by ISO and ITU-T as standards recognized by them as treaty-based standards bodies.

Exhibit B to this letter elaborates on the four open questions raised by the CPPB on August 22, 2025. The comments here benefit from a consensus opinion from the US & Canada Open Banking Subgroup, comprised of US and global experts from the FAPI Working Group and Ecosystem Support Community Group.

We hope these comments are material and useful in your deliberations. We welcome further discussion on our comments, and you can reach us directly at director@oidf.org to organize a discussion.

Sincerely,

Gail Hodges
Executive Director
OpenID Foundation

CC: NIST - Director Craig Burkhardt(craig.burkhardt@nist.gov)

Exhibit A. Ecosystems Selecting FAPI (non-exhaustive list)

Ecosystems	Public Sector or Private Sector Led	Selected FAPI	Require FAPI	Deployed FAPI
US Financial Data Exchange - Open Finance - FAPI 2.0 is the approved "blue" profile	Private sector led	◉	◉	◉
United Kingdom - Open Banking	Government sector led	◉	◉	◉
Australia - Treasury, Data Standards Body, Open Data	Government sector led	◉	◉	◉
Australian - ConnectID (identity data, bank-led consortia)	Private sector led	◉	◉	◉
Brazil Open Finance	Government sector led	◉	◉	◉
Saudi Arabian Monetary Authority - Open banking	Government sector led	◉	◉	◉
United Arab Emirates - Open Banking	Government sector led	◉	◉	◉
Chilean Ministry of Finance - Open banking	Government sector led	◉	Expected 2026	Expected 2026
Colombia - Open banking	Government sector led	◉	Expected Nov 2025	Expected Nov 2025
Norwegian HelseID - Health data, OIDF/ HelseID blog post	Government sector led	◉	◉	◉
German Verimi - (private, open banking consortia)	Private sector led	◉	◉	◉
Canada - Open Banking	Government sector led	Expected	Expected	Expected

Notes:
(1) Other G20 and global south countries have selected FAPI 2.0, but it is confidential to OIDF, not yet public information.
(2) OIDF is an observer to the Bank of International Settlements "Aperta Project," given the fit of FAPI 2.0 to support supply chain and transaction banking use cases.

Exhibit B: OpenID Foundation comments on CFPB-2025-0037, « Personal Financial Data Rights Reconsideration »

1. The proper understanding of who can serve as a "representative" making a request on behalf of the consumer;

The OpenID Foundation does not seek to prescribe which specific entities may serve as a consumer's "representative," given the OIDF is not a governance body, and the definition of who and what may act as a "representative" could evolve over time and would be defined by a local jurisdiction. OIDF specifications and standards can be selected and deployed independent of who the CFPB designates as "representatives."

2. The optimal approach to the assessment of fees to defray the costs incurred by a "covered person" in responding to a customer driven request;

As a technical, open standards body, the OpenID Foundation is not privileged to information from our members (government entities or private entities) on the operations of their ecosystems and businesses. However, as experts supporting 12 ecosystems for 5+ years, we have observations for the CFPB's consideration.

One of the most persistent challenges in open banking regimes around the world has been how to fund the infrastructure that makes secure, consumer-directed data sharing possible and commercially sustainable for all stakeholders. In nearly every market, the initial instinct has been to require banks and other data holders to bear the full cost of compliance — a decision that can spur early adoption but becomes increasingly difficult to sustain as ecosystems grow in scale and complexity. Banks in the U.K., Australia, Brazil and elsewhere were required to stand up secure APIs, consent dashboards, and monitoring infrastructure without charging third parties for access. This model accelerated the first wave of innovation, but as consumer demand grew — often resulting in millions of high-frequency API calls per day and billions of calls per months— costs shifted heavily and permanently onto data holders. The result has been mounting pressure to introduce fees, often in an ad hoc and reactive way, creating unpredictability and, in some cases, discouraging further investment.

Brazil's Open Finance framework conceptually allows for regulated charging, but in practice the option has rarely been exercised because the largest banks have also become the largest third-party providers. Nevertheless, the principle that all participants contribute to sustaining the ecosystem has been foundational. It has directly informed the commercial structures of networks that build on the same technical and trust foundations — including Australia's AP+ ConnectID and New Zealand's Get Verified fraud-prevention network — both of which have demonstrated that when cost is distributed in proportion to participation and benefit, innovation can scale without compromising security.

Having observed these challenges, the OIDF suggests that the CFPB consider a clear, principle-based framework for cost recovery from the outset.

Such a framework should recognise two realities:

1. it is not fair or sustainable for covered institutions to subsidise unlimited API access indefinitely;
2. but (if competition is an important objective of the regulator) it is equally important to avoid pricing that creates artificial barriers to entry or entrenches the largest players.

Two objective drivers dominate infrastructure cost:

- the frequency of data calls
- the number of distinct consumer records under management.

In our observation, the most effective cost models internationally tie fees to actual usage rather than fixed licence or “access” charges.

Low-volume, low-risk use cases — for example, a budgeting app pulling a single account balance once a day — might remain free or priced at a nominal level to encourage innovation and inclusion. High-frequency or complex use cases — such as continuous account monitoring, analytics engines, or payment initiation at scale — can justifiably attract fees that rise with usage. In some instances the higher frequency or complex use cases are referred to as “premium” services.

This approach has several advantages. It gives new entrants a path to market without prohibitive upfront costs. It allows banks to invest in secure, scalable infrastructure knowing that heavy or premium users will eventually contribute to sustaining it. And it makes costs transparent and predictable for fintechs building business models on top of open banking access. Crucially, it avoids the opaque pricing power that can occur if each data holder sets its own bespoke fees.

Across these jurisdictions, successful cost-recovery approaches share several characteristics:

- **Usage-linked fairness:** Fees, where applied, relate to measurable activity such as the frequency of API calls or number of consumer records accessed, ensuring low-risk and low-volume use cases remain free or nominal while heavy users contribute proportionately.

- T**ransparency and predictability**: Published, regulator-reviewed schedules create certainty for all market participants and deter anti-competitive or exclusionary pricing. In markets where the regulator does not perform this function, a regulated entity or industry group could achieve the same objective.

- **Sustainability through shared obligation**: Even in markets where direct charging is limited, an accepted understanding that infrastructure must be collectively maintained has encouraged ongoing investment in resilience and performance.

The economic evidence from Brazil, Australia, and the U.K. also illustrates that open technical standards play a central role in keeping overall costs manageable. Frameworks based on the Financial-grade API (FAPI) 2.0 profile have consistently lowered implementation costs by removing the need for bespoke security development and by enabling shared certification and testing services. We elaborate on the benefits of FAPI, from a security and operating perspective.

Ultimately, sustainability depends less on the presence or absence of specific fees and more on the clarity and balance of the model itself. Ecosystems in which all participants understand that maintaining a secure, high-trust environment involves both financial and operational responsibility have remained more stable, innovative, and consumer-focused over time.

3. The threat and cost-benefit pictures for data security associated with section 1033 compliance

Digital access to personal financial data is not new in the United States. Banks already expose customer information through web portals, mobile apps, and APIs — sometimes for their own channels, sometimes for select partners. Section 1033 is not about creating access where none exists; it is about ensuring that data sharing serves consumers' interests and meets consistent security, reliability, and affordability baselines as use cases expand.

The security risk lies not in opening data up for access and data sharing, but in <u>how</u> it is opened. Fragmented or ad hoc API implementations create uneven attack surfaces, duplicated security investment, and weak links that sophisticated actors exploit. Legacy OAuth 2.0 alone, for example, has documented shortcomings in high-risk financial contexts: token replay, authorization code injection, and session fixation attacks are well known and actively exploited when implementations diverge or cut corners. Each proprietary variation becomes an unpredictable point of failure, as noted by JPMC CISO Patrick Opet in his letter to SaaS providers:

- Software providers must prioritize security over rushing features. Comprehensive security should be built in or enabled by default.
- We must modernize security architecture to optimize SaaS integration and minimize risk.
- Security practitioners must work collaboratively to prevent the abuse of interconnected systems.

Source https://www.jpmorganchase.com/about/technology/blog/open-letter-to-our-suppliers.

We have helped many ecosystems globally to accomplish the outcomes Patrick Opet is seeking, in the domain space of Open Banking, namely to deploy FAPI across all ecosystem participants and supports its evolution over time as the ecosystems evolve. We have worked in partnership with the Financial Data Exchange in their journey to adopt FAPI 2.0 as the "blue" security profile. We would be happy to explain the benefits of FAPI 2.0 to the CFPB in more

detail, and help explain how even wider or comprehensive adoption could benefit the US ecosystem. The following sections offer key themes to that effect.

Why FAPI 2.0 Delivers on Security by default

FAPI 2.0 is the first API security profile built with a formal attacker model, developed in collaboration with leading academic cryptographers and cyber security researchers. It explicitly addresses modern threats such as token replay, credential theft, and transaction manipulation. Its safeguards — sender-constrained tokens, signed authorization requests, granular consent, and proof-of-possession access tokens — have been demonstrated working in production at national scale in the U.K., Australia, Brazil, Saudi Arabia and the UAE. It represents a mature, evidence-based baseline rather than a theoretical or bespoke approach.

Systemic security benefits of a single FAPI 2.0 profile

When all participants implement the same advanced security profile, the weakest-link problem is dramatically reduced: attackers cannot simply target the least-protected bank or fintech because each conforms to a hardened baseline. At the same time, it is important to acknowledge that a single common protocol also creates a shared-risk surface — if a vulnerability exists in that protocol, it could in theory affect the entire ecosystem.

This is precisely why open standards bodies and transparent governance matter. Protocols like FAPI 2.0 are not controlled by any single vendor; they are developed and maintained in open technical communities where banks, fintechs, vendors, academics, and security experts all collaborate. Vulnerabilities are handled through responsible disclosure programs, public tracking, and coordinated updates. Because the specification is public and continuously scrutinized, weaknesses are usually discovered and addressed more quickly than in fragmented, proprietary models where each institution builds and patches its own unique approach in isolation.

Opaqueness serves no one: it hides risks, delays collective response, and leaves consumers exposed to silent failures. A unified, openly governed protocol like FAPI 2.0 creates the opposite dynamic — early visibility, shared expertise, and rapid, ecosystem-wide remediation — ensuring that when a flaw is found, it is fixed once and deployed everywhere. By “locking arms” as a US and global community, we reduce the window of opportunity for attackers, and address the well-informed concerns of experts like the JPMC CISO.

The economic advantages of a single FAPI 2.0 profile

Markets that have converged on a single advanced profile have seen lower implementation and maintenance costs over time. In the U.K. and Australia, once FAPI self-certification became the common denominator, vendor support matured, reusable components proliferated, and conformance testing was automated. Banks avoided the cost of custom code for every integration; fintechs could integrate once and reach many data holders; regulators gained a clear, auditable compliance target and all stakeholders benefit from the clearly defined security properties, industry stakeholder and academic review, industry and the successful operational

implementations. Conversely, markets that left security optional or vendor-defined have struggled with duplicated spend, inconsistent user experience, and vulnerability remediation.

Regulatory / Managing Entity advantages of a single FAPI 2.0 profile

When regulators or local “managing entities” advocate for or require a single, certifiable security profile like FAPI 2.0 it simplifies supervision. Instead of the CFPB or its regulated entity auditing thousands of unique implementations, the Bureau can require periodic independent certification to a single global baseline, much as other regulators have done. This moves compliance from a subjective “checklist” exercise to a transparent, empirically testable standard.

It is important to note that many private sector ecosystems choose to policy that FAPI 2.0 is required to implemented by both data holders and date recipients, and to regularly establish conformance to FAPI 2.0. They do so for many of the same reasons that their peer decisions makers in government-led ecosystems require use of FAPI 2.0. When conformance is required in either case, the usual policy is annual self-certification of conformance, and the best practice is to also run ongoing real time tests to ensure connectivity is not broken amongst any implementers in the ecosystem.

Last but not least, decision makers concerned with their ability to interoperate across borders are also swift to adopt standards that improve their competitive position. By FDX adopting FAPI 2.0 in the US, they open the door to U.S. international interoperability — important as US businesses seek to engage with consumers in other markets where FAPI 2.0 is the defacto choice.

The Innovation Advantages of a single FAPI 2.0 profile

Aligning Section 1033 with FAPI 2.0 does more than reduce risk: it helps covered institutions seize innovation more easily. They can modernize existing digital channels, retire legacy security debt, and compete on user experience and product features rather than competing on security features or on the basics of interoperability with counterparties. Taking it a step further, it creates a shared foundation for future innovation — advanced consent dashboards, richer payment initiation, and privacy-preserving analytics — extension points for adding functionality - without forcing each institution to reinvent secure transport between the ecosystem participants.

Without this direction, the U.S. risks repeating mistakes seen elsewhere: fragmented security models, higher cumulative cost, and persistent breach exposure that undermines consumer confidence. By adopting a single, rigorously analyzed standard such as FAPI 2.0 and requiring regular certification, the CFPB can lift the entire ecosystem’s resilience and trustworthiness while keeping long-term compliance costs predictable.

Central role of Accreditation and Conformance

Our recommendation is that the US market establish a single, accreditation process that applies uniformly for to ensure the optimal security outcomes are achieved, based on two principles:

1. That any eligible and qualifying representatives should be approved as a pre-requisite for participation in the ecosystem

2. That the representative approval should be a transparent, predictable, and enforceable process.

Experience from other open banking regimes shows why this matters. When conformance and accreditation is left predominantly to private entities, large incumbents can often leverage their market position to set terms favorable to themselves and leading to market distortions. For example, smaller institutions and new entrants may face high and/or inconsistent costs, integration becomes selective so coverage is porous, and consumers at smaller /regional institutions may be left behind.

A well-designed scheme would apply the same core principles to every participant, and calibrate its requirements to the sensitivity of the data and the impact of the services offered.

Lower-risk use cases — such as simple read-only data access — could be supported by a lighter accreditation process, while higher-risk activities such as initiating payments or holding persistent access to financial transactions would require more rigorous security, privacy, and governance controls. Decisionmakers must therefore strike a careful balance: proportionate to risk, predictable in cost and effort, and capable of evolving as the market matures.

Technical requirements should be objective and testable with conformance tools

For example, proving technical conformance to the FAPI 2.0 profile reduces subjective judgment and implementation costs for all parties. Nearly all the ecosystems we work with use our free, open source tests to ensure implementers in their ecosystem have implemented correctly to the standards. This serves their own self interests to realize the security, interoperability, operational scale and consumer-consent features inherent in the FAPI 2.0 security profile. Beyond the protocol, transparency, due process, and public registers of accredited parties are essential so that participants understand the rules and consumers know who is trustworthy. It also ensures that any implementing entity does not need billions of dollars of IT infrastructure and people resources in order to ensure a common high bar for security available to all ecosystem participants. In Brazil for example, small co-operative banks in the “long tail” of deploying entities implement to the same requirements as the largest financial leaders in the market.

To further support managing entities like the Financial Data Exchange, the Board announced the intent to launch an accreditation program so that other entities can operate their own conformance capabilities inclusive of OIDF tests and best practices:https://openid.net/oidf-announces-new-investment-to-expand-conformance-services/

Align ecosystem rules with Conformance

Critical to open banking and open data ecosystem success is the capacity to evolve over time, and make timely adjustments. Other markets provide clear lessons. The United Kingdom

achieved strong early coverage among its nine largest banks but left many smaller institutions and their customers underserved because the accreditation and integration was fragmented and bilateral amongst smaller tier entities. Australia took the opposite path, creating a robust consumer rights framework but initially imposing an accreditation process so heavy that it discouraged small innovators and slowed ecosystem growth. The U.S. can avoid both pitfalls by defining a conformance framework that is risk-based and proportionate from the outset, and which is inclusive of technical requirements from across the ecosystem, and that can evolve as the ecosystem, technologies, and use cases mature.

AI & Open Banking is the Next Frontier… and it is already happening

Technology and use cases continue to evolve, but few shifts have been as rapid or consequential as the rise of **Agentic AI** — systems that act on behalf of individuals or institutions. These agents introduce new ways for consumers to engage with financial services and, at the same time, new categories of operational and security risk.

Across multiple markets, a familiar pattern is re-emerging. AI-driven agents are beginning to scrape financial data at scale, storing serialised credentials or identity tokens in insecure environments and initiating transactions without robust consent frameworks. It mirrors the problems that pre-dated Open Banking: unverified access, weak authentication, and opaque data use.

The OpenID Foundation's recent **AI & Identity Whitepaper** analyses this trend and concludes that the same safeguards that underpin Open Finance — strong authentication, proof-of-possession credentials, verifiable consent, and continuous certification — are precisely the safeguards required for the responsible operation of Agentic AI.

https://openid.net/new-whitepaper-tackles-ai-agent-identity-challenges/

In this light, secure Open Finance infrastructure should be viewed as a strategic upgrade for all digital channels, not a narrow compliance exercise. The same architecture that protects consumer-permissioned data also secures future AI interactions, partner integrations, and embedded-finance models. **FAPI 2.0** and related specifications embed these controls directly into the communication layer, ensuring every request carries non-repudiation, authenticated provenance, and explicit consumer consent.

Australia's experience with AI + FAPI offers a preview of what comes next.

Having built consent and accreditation frameworks through the Consumer Data Right, Australian banks are now aggressively embracing AI — not as an experiment but as a new primary engagement channel. Executives increasingly view intelligent agents as the interface through which most customers will eventually interact. What was once speculative in Open Finance is now being treated as a near-certainty by globally systemically important banks.

Because these institutions already operate on FAPI-based security and trust frameworks, they are free to innovate safely: deploying AI-driven advisory services, conversational banking, and

automated decision-making while maintaining consistent fraud prevention and auditability. This same foundation — secure consent, federated identity, and certified interoperability — serves every distribution model, whether the user is a person, a partner, or an algorithm.

Those without these controls face a different reality. As fraudsters adopt AI tools, attacks now occur at AI scale: generating synthetic identities, imitating legitimate behaviour, and exploiting inconsistent API defences faster than any manual system can respond. It has become an arms race between automation and assurance. In that context, ecosystems built on standards such as FAPI 2.0 hold a decisive advantage, embedding integrity, accountability, and consumer authorisation directly into each interaction.

By upgrading their core infrastructure now, financial institutions are not only meeting the requirements of Open Finance but building the secure substrate for the next decade of digital engagement — one that enables innovation at the speed of AI without surrendering control, consent, or consumer trust.

Standards are vital to mitigate the cybercrime threats to Americans and American businesses.

Fraud is not a peripheral issue for Open Finance; it is a core public-interest and national-security concern. According to the Aspen Institute's National Strategy for Fraud and Scams, Americans lose more than $150 billion each year to scams. The report underscores that consistent, open standards are essential to strengthening the country's digital and financial resilience.

Every jurisdiction that has implemented open finance has learned the same lesson: fraud is everyone's game. Once connectivity increases, bad actors look for inconsistency — the seams between different banks, APIs, or consent models. The ecosystems that have responded most effectively have done so by building fraud-mitigation overlays on top of shared, standardized trust frameworks.

New Zealand provides a clear example. When regulators mandated that banks deliver a unified solution for the *Get Verified* ecosystem — based on FAPI 2.0 and the same open-banking architecture seen elsewhere — the industry stood up a Confirmation of Payee (CoP) service in less than six months. The benefits have been immediate and measurable:

- The Banking Ombudsman reported a 17 percent year-on-year drop in scam-related complaints — the first decline after several years of steady increases.

- ANZ New Zealand recorded a 30 percent reduction in misdirected payments, reducing operational burden and strengthening trust in the payment system.

These results demonstrate that when an entire market delivers a single, unified solution built on common standards, defensive capabilities can be deployed quickly and at scale. The same

foundation now allows New Zealand's institutions to extend their fraud-reduction initiatives further with minimal friction.

Globally, the pattern is consistent. Where ecosystems adopt a certifiable, uniform baseline such as FAPI 2.0, each participant becomes more resilient — and collectively, they gain the ability to share risk signals, detect coordinated attacks, and respond faster. Standards don't just make security cheaper; they make collaboration possible.

A U.S. Open Finance framework grounded in interoperable, testable standards can follow this proven trajectory: enabling innovation while providing the foundation for collective defense. The lesson from abroad is clear — single, unified solutions built on open standards make whole-of-market fraud reduction achievable, quickly, and with measurable impact.

Global Standards & US leadership in Open Finance.

The US has been a thought leader in Open Finance for ~10 years, but its market leader advantage is at risk. The US market size makes a four party model a market reality, however three party models prevail in other jurisdictions. As 90+ countries pursue open finance (a key pillar of the Digital Public Infrastructure movement supported by the G20), they are leaning towards the use of proven global open standards like FAPI 2.0, and also have a bias to government led models and 3-party models. FAPI 2.0 works for a three party and a four party mode. That said for implementers in the US not using the blue profile/FAPI 2.0 (e.g. the "Green" profile) those implementers will have a rough path to cross border interoperability outside of the US and Canada. If the US wants to be a leader in the global landscape, it will need to scale the use of global open standards like FAPI.

Competition over the cargo not over the railway dimensions

Security should not be the dimension on which competition is encouraged. In one G7 country example, a bank actively encouraged a lower security bar so that their deployment would be more secure and bad actors would pursue their competitors and their consumers. In US open banking, decision makers have the option to encourage competitive dynamics that incentivise a level playing field, where any qualified party can participate by meeting the same published security standards, and all consumers — regardless of where they bank — can benefit from the same protections and access to the same services.

It is easy for decision makers to do too much or too little when setting rules

The OIDF appreciates that the CFPB's task of achieving desired outcomes is not straightforward - it is easy to go too far or do too little. If the obligations on participants are set too high, innovation stalls and smaller participants are effectively shut out. This is a challenge we observed in Australia when its Consumer Data Right launched with a single, heavy accreditation hurdle that was cost-prohibitive and undermined adoption. If the bar is set too low or does not exist, then consumer protection is weakened and trust in the system erodes. Open banking ultimately thrives only if it is trusted — and remains trusted long enough to become an everyday utility.

4. The threat picture for data privacy associated with section 1033 compliance.

Financial data sharing already occurs at scale in the United States, yet much of it still relies on broad, opaque, and effectively irreversible permissions. In the worst cases, consumers often grant third parties wide-ranging access to their accounts through screen scraping or legacy APIs, with few tools to see or control what data is shared, for how long, or for what purpose. The resulting “consent fatigue” erodes trust and increases cumulative privacy risk as data is reused beyond its original intent.

Experience from other jurisdictions demonstrates that trust improves when consumers are given clear, time-bound, and auditable control over how their data is used. Modern open-data ecosystems have achieved this balance by pairing technical standards that enable fine-grained permissions with governance frameworks that define and enforce how those permissions are applied.

Technical enablement: granular and revocable consent

The Financial-grade API (FAPI) 2.0 family, together with technical specifications such as Rich Authorization Requests (RAR) and Grant Management, provides the technical basis for fine-grained, purpose-bound, and revocable consent.

• RAR allows a third party to request precisely the data it needs — for example, “90 days of checking-account transactions” — while specifying the intended purpose and duration.

• Grant Management APIs give consumers a live, standardized view of every permission they have granted, allowing them to amend or revoke access in real time across multiple services.

When these specifications are implemented, each authorization event is expressed in machine-readable form, providing both consumers, oversight organizations and (where relevant) regulators with a verifiable record of what was accessed, by whom, and under what terms.

These mechanisms have been implemented across the United Kingdom, Australia, Brazil, and the United Arab Emirates, giving consumers predictable controls and regulators traceable oversight. They have shown that privacy assurance and innovation are not mutually exclusive when consent is made specific, auditable, and easily withdrawn.

The policy dimension: enabling versus enforcing minimization

While these standards make data minimization and purpose limitation possible, they do not enforce them automatically. A third party could still request more data than necessary unless governance rules define what is reasonable and proportionate. Other jurisdictions have found

that pairing open technical standards with clear operating rules — defining permissible scopes, acceptable use, and penalties for misuse — is essential to achieving real privacy outcomes.

In Australia's Consumer Data Right and Brazil's Open Finance program, purpose-bound consent is both technically expressed and legally circumscribed: over-collection is treated as non-compliance. This blend of protocol and policy has created demonstrable consumer confidence while keeping participation open to a wide range of providers.

Operational governance and ecosystem alignment

Operating entities such as the Financial Data Exchange (FDX) in the United States are well placed to develop and maintain the practical rulebooks that complement these global technical standards — establishing consistent consent screens, data-usage reporting, breach-handling procedures, and consumer redress mechanisms. Where FAPI 2.0 and RAR provide the plumbing, such operating rules form the guardrails that ensure privacy expectations are met in practice. Just as discussed in the security contest, the same is true to privacy, managing entities like FDX have the operating flexibility to adapt and evolve as the marketplace evolves.

Global lessons on privacy and trust

Open-banking ecosystems that have combined granular consent protocols with enforceable minimization principles — notably the U.K. and Australia — have seen measurable gains in consumer participation. Those that relied on broad, indefinite permissions have struggled to build durable trust. Emerging markets such as the UAE have embedded these lessons from inception, incorporating both privacy-by-design architecture and continuous certification into their frameworks.

A balanced model for the United States

Evidence from these implementations suggests that the most sustainable approach is one where technical capability and regulatory clarity reinforce each other. Standards like FAPI 2.0, RAR, and Grant Management supply the mechanisms for precision, transparency, and revocation; consistent oversight paired with conformance/accreditation mechanisms and clear enforceable operating rules ensure that those mechanisms are applied fairly and proportionately. Together they enable an ecosystem in which consumers can participate confidently, innovators can operate predictably, and privacy becomes a practical foundation for competition rather than a compliance burden.