The CFPB's Section 1033 Rule Is Not an 'Open Banking' Rule

Paige Pidano Paridon & Austin Anton | Dec. 19, 2024

The Consumer Financial Protection Bureau recently finalized new rules dictating how certain banks and other "data providers" – institutions offering deposit, savings, prepaid accounts or credit card accounts, as well as digital wallet providers – must share certain consumer financial data. Section 1033 of the Dodd-Frank Act obligates financial institutions to make a consumer's financial data available to the *consumer* upon their request pursuant to rules issued by the CFPB. Some have mischaracterized this rule as ushering in "open banking" in the U.S. While the term open banking continues to mean different things to different people, in different areas of the world, neither the statutory language nor the intent behind the law suggests that Congress intended to create open banking through Section 1033. The statutory provision is only about 300 words, stating "…a covered person shall make available **to a consumer**, upon request, information … concerning the consumer financial product or service that the consumer obtained from such covered person …"[1]

Any notion that this is, or was intended to be, open banking distorts the statute and Congressional intent, and ignores the key principles of open banking.

What is "Open Banking"?

Open banking generally aims to improve consumer convenience and ignite competition by making it easier for consumers to share their financial data with other companies, generally other financial institutions. If data is in the same format, it is easier to transfer between systems, thereby enabling companies to use that data to launch new products and services and giving consumers the ability to change banks with greater ease.

More than 20 unique models of open banking have emerged around the world, each varying in structure

[1] https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title12-section5533&num=0&edition=prelim

and maturity. Some models are market-driven and largely voluntary, such as Singapore's and, prior to Section 1033, the United States'. Others are government-led with strong regulatory backing and defined technical standards, as seen in the European Union and the United Kingdom. Despite their differences, open banking frameworks generally reflect three key principles:

1. **Data Standardization**– establishing consistent data formats and protocols for easy sharing and creating rules to resolve conflicts between participants;
2. **Consumer Safety, Consent and Disclosure** – protecting consumers from bad actors and ensuring those consumers have a say over who accesses their data; and
3. **Data Access, Use and Retention Restrictions** – setting limitations on who has access to data and how third parties use and save data after obtaining permission.

Open banking is a subset of a much broader global trend to make data standardized and accessible for both research and commerce (*see* Data.gov). However, open banking is not tantamount to "open payments," where the goal is to give third parties, including fintechs, access to consumers' bank accounts to facilitate financial transfers from point A to point B, nor is it tantamount to "open finance," a broader concept that involves data sharing between banks and any other third party, such as insurance companies, data aggregators, investment firms and other nonbank lenders. While Congress did not intend Section 1033 to be an open banking mandate, it is informative to look at how other jurisdictions have approached these three primary principles of open banking in considering how the CFPB's 1033 rule compares.

A Global Comparison: U.S. vs. International Models

The three open most frequently cited overseas counterparts to Section 1033 include Australia, the European Union and the United Kingdom.

Australia's model is regulated by the Office of the Australian Information Commissioner and the Australian Competition and Consumer Commission. Among the three foreign jurisdictions, Australia's framework is most comparable to the CFPB's Section 1033 rule because it primarily focuses on the ability to access and share financial data. Only recently did Australia expand its rules to include payment initiation requirements, enabling third parties to facilitate payments to and from bank accounts on behalf of a consumer (i.e., "open payments").

The E.U. and U.K. models were adopted before Brexit and, as a result, share many similarities. The E.U. model is governed by the European Banking Authority and authorities in each member country. The U.K. model is governed by the Financial Conduct Authority and the Competition and Markets Authority. Both jurisdictions, and relevant statutes, explicitly prioritize *open payments*, with open banking serving as a secondary objective. The European Union only recently finalized the Financial Data Access Regulation (FiDA), which will aim to achieve open banking *and* open finance when it takes effect in 2027. It's worth noting that the E.U. authority stems from the revised Payment Services *Directive* (PSD2), not a regulation; therefore, member countries can (and do) have country-specific requirements.

Criteria	United States	Australia	Europe	United Kingdom
Legal Authority	Dodd-Frank Act Section 1033 (Personal Financial Data Rights)	Consumer Data Right Act (Amendments to the Competition and Consumer Act 2010 and the Privacy Act 1988)	PSD2 (Directive; Not Regulation); National Competent Authorities in Each E.U. Jurisdiction; Financial Data Access Regulation (FiDA)	Payment Services Regulations (2017) Retail Banking Market Investigation Order (2017)
Primary Regulator	CFPB	Office of the Australian Information Commissioner (OAIC); Australian Competition and Consumer Commission (ACCC)	European Banking Authority; National Competent Authorities in Member Country Jurisdictions	Financial Conduct Authority; Competition and Markets Authority

How does the CFPB's 1033 rule hold up to the principles of open banking?

Principle #1: Data Standardization

The first principle of open banking is obtaining consistent data. Most jurisdictions tackle this goal by either establishing technical standards or by designating a single, universal standard-setting body. Section 1033 does neither.

The CFPB's final rule allows standard-setting bodies to apply for recognition. Once an application is submitted, the CFPB conducts a review and has the option to solicit public feedback. The CFPB has yet to recognize any standard-setting body. However, the non-profit Financial Data Exchange was the first to apply. FDX was established in the U.S. and Canada in 2018 and currently serves as a voluntary standard-setting body among banks, financial institutions, data aggregators and consumer groups, with broad representation by over 230 different stakeholders. FDX has developed a technical specification for secure data sharing via API that is regularly updated and currently connects to more than 94 million consumer accounts. While FDX is already well established in North America, Section 1033 could lead to multiple standard-setters operating in the U.S., which may result in CFPB-induced confusion and divergent standards. Moreover, the final 1033 rule does not mandate that third parties use secure interfaces or share data in a standard data format, thereby undermining one of the key benefits of open banking.

Both Australia and the U.K. have a single standard-setting body governing data standardization, Consumer Data Standards in Australia and the Open Banking Implementation Entity (OBIE) in the United

Kingdom. While there is no single-standard setting body established under the E.U. directive, PSD2 includes Regulatory Technical Standards that outline core principles. As a result, E.U. member states designate their own standards based on these expectations (e.g., XS2A [Germany]; STET [France], PolishAPI [Poland]).

Data standardization and "open banking" *should* naturally lead to data reciprocity. Meaning, fintechs, including data aggregators, that obtain data from data providers are also obligated to share data with the data provider (i.e., the bank), as is the case in Australia and the E.U. That is largely not the case in the United States or the United Kingdom.

The Verdict: *Fail*. Section 1033 doesn't hold up to data standardization principles because it does not establish clear, universal standards or mandate that third parties use secure interfaces or standardized data formats. While it seeks to recognize standard-setting bodies, organizations like FDX were already doing the work to develop technical specifications for secure data sharing, and the rule could undermine this progress should the CFPB designate more than one standard-setting body that would each establish different versions of standardized data sharing formats.

Criteria	United States	Australia	Europe	United Kingdom
Universal Technical Standard-Setting Body	No.	Yes.	No. (See Appendix A.)	Yes.
Requires Data Recipients (i.e., Fintechs) to Reciprocate Data Sharing with Banks	Partially. Digital wallet providers are in scope, others are not.	Yes.	Yes.	No.

Principle #2: Consumer Safety, Consent and Disclosure

The second principle of open banking is giving consumers control over their data by, for example, ensuring that consumers know what they are sharing, with whom they are sharing it and how the data is used. Moreover, consumer data should remain safe and secure regardless of where the data resides. Importantly, there should be data security, consumer protection and other requirements imposed on data recipients and oversight over those entities to ensure that they are following the rules. While all four jurisdictions require third-party providers to acquire consumer consent and reobtain consent after a certain amount of time (e.g., 12 months in the U.S.), the rules vary significantly regarding the requirements imposed on third parties and whether and how they are subject to oversight.

In addition, many other jurisdictions have taken significant steps to ban unsafe practices like screen scraping, which gives fintechs and other third-party providers consumers' sensitive credentials like usernames and passwords, which in turn provides them unfettered access to all of the consumers' account data, well beyond the data needed for a particular product or service.

The U.S. does not prohibit screen scraping, require robust data security protections, or generally provide for regulatory oversight of third-party data recipients. Notably, the final 1033 rule mandates the sharing of payment initiation information, such as account and routing numbers, which are highly sensitive, and

could be used by criminals to drain a consumer's account. Without proper requirements imposed on, and oversight of, third parties, the chances of bad actors gaining access to data from third parties with weak security practices increases. Furthermore, the likelihood of fraud and scams could increase if banks are prohibited from appropriately protecting their customers by restricting third parties' access to their customers' sensitive information like account and routing numbers based on banks' risk management assessments.

By contrast, regulators rightfully fulfill their oversight responsibilities in overseas jurisdictions. The Financial Conduct Authority directly oversees fintechs in the U.K. The Office of the Australian Information Commissioner and the Australian Competition and Consumer Commission serve that role in Australia. In the E.U., payment service providers must carry out an annual assessment of their operational and security risks. Third-party providers also receive different regulatory treatment depending on their business model and perceived risk level of the underlying activity. For example, the E.U. bases the stringency of its rules and regulations on the third party's business (i.e., whether the third party is an account-servicing payment service provider (e.g., banks, credit unions), payment initiation service provider (e.g., payment companies like Visa, Mastercard, Stripe), account information service provider (e.g., aggregators like Plaid, Yodlee) or financial information service providers (e.g., data *users* such as Empower, or other fintech apps)). Australia and the U.K. have similar distinctions. The CFPB has instead elected to take a back seat.

Additionally, when a third-party provider suffers a breach or data is shared without authorization, every jurisdiction *except the U.S.* has rules to clearly apportion liability and responsibility. If a U.S. bank shares data with a fintech and that fintech suffers a data breach, the bank could still be liable even if the consumer authorized the request. This failure to explicitly require liability of third parties further disincentivizes those entities from implementing appropriate data security controls, making consumers' sensitive financial data vulnerable to theft and misuse by criminals.

The Verdict: *Fail*. While Section 1033 requires consent and disclosure, it does not meet core requirements for protecting consumers, maintaining data security, or overseeing third parties.

Criteria	United States	Australia	Europe	United Kingdom
Prohibits Screen Scraping	No.	No.	Significant steps to ban screen scraping.	Significant steps to ban screen scraping.
Requires Fintechs to Register and Obtain Accreditation	No.	Yes.	Yes.	Yes.
Regulations Differentiate Banks from Nonbanks	Yes.	No.	No.	No.
Regulators Take Responsibility to Supervise and Examine Fintechs	No.	Yes.	Yes.	Yes.
Clear Liability Apportionment	No.	Yes.	Yes.	Yes.

Criteria	United States	Australia	Europe	United Kingdom
Between Data Provider and Data Recipient				

Principle #3: Data Access, Use and Retention Restrictions

The third and final principle of open banking is establishing clear rules around who can access data, the types and scope of data that can be accessed, how it can be used and how long it can be retained.

Australia, the E.U., the U.K. and the U.S. have established specific criteria for eligible financial data, including transaction details, account balance information and upcoming bill data, among others. These frameworks also aim to minimize the amount of data collected by requiring that only the data necessary to provide the consumer's requested product or service may be collected. In addition, these jurisdictions require that financial data is used only for its intended and authorized purpose — such as enabling a payment transaction — rather than for unrelated activities like targeted marketing. However, as noted throughout, the CFPB has declined to subject third-party data recipients to regulatory oversight as part of the final rule. Therefore, the CFPB failed to give itself the authority to proactively monitor these entities' data security practices and thereby potentially prevent data theft or other misuse before they occur.

Australia, Europe and the United Kingdom also all require fintechs to meet strict technical and safety standards and obtain accreditation before they are permitted to access consumer financial data. The U.S. does not, and no such certification is offered. Under the CFPB's new rule, *any* fintech can request data from a bank if the consumer authorizes the request – no accreditation is required. There are few safeguards in place to prevent an unsafe fintech from seeking access to consumer data, and the determination of what constitutes unsafe is largely undefined. The rule limits banks' ability to deny access to third parties on risk-management grounds.

The Verdict: *Partially Achieved*. Section 1033 imposes data minimization requirements and secondary use limits, but provides limited and inconsistent oversight mechanism to ensure third parties abide by those limits. Moreover, it requires banks to share sensitive account data and limits their ability to restrict access based on risk management concerns.

Criteria	United States	Australia	Europe	United Kingdom
Requires Banks to Share Sensitive Payment Initiation Data (e.g., Account and Routing Numbers)	Yes.	Yes.	Yes.	Yes.
Allows Banks to Deny Access to Unsafe Third Parties	Unclear.	Yes.	Yes.	Yes.

Criteria	United States	Australia	Europe	United Kingdom
Secondary Use Limitations/Data Minimization Requirements	Yes.	Yes.	Yes.	Yes.

The Final Verdict: Section 1033 is Not Open Banking

The CFPB's finalized Section 1033 rule attempts to create a framework for consumer data-sharing but meets only one of three key principles to achieving open banking. The rule fails to address critical elements of security and oversight and while it takes a step toward standardizing access and data usage, it falls short compared to overseas models in several key areas:

- **Security and Oversight Gaps**: Unlike Australia, the E.U., and the U.K., the U.S. rule lacks meaningful accreditation requirements for fintechs, does not prohibit unsafe practices like screen scraping, and leaves banks to police third-party safety.
- **Liability Apportionment**: Section 1033 fails to establish clear rules for apportioning liability between banks and fintechs for covered data in the event of data breaches or fraud, placing undue responsibility on banks.
- **Universal Standards and Reciprocity**: While the rule contemplates the use of standard-setting bodies like FDX, the rule does not create a universal standard or enforce data reciprocity, creating a one-way pipeline for data to flow and undermining the basic tenets of open banking, leaving an uneven marketplace.
- **Mixing Open Banking and Open Payments**: By attempting to combine open banking and open payments into a single rule, without appropriate guardrails, the CFPB creates a fragmented framework that increases the likelihood of fraud and scams and data misuse.

Section 1033 threatens to disrupt a market-driven, consumer focused ecosystem that already enables billions of secure data transfers every month — an ecosystem that works precisely because it prioritizes both security and consumer choice. Open banking cannot be achieved by simply calling it so, and despite its framing, the U.S. model does not achieve this goal, likely because Congress never intended Section 1033 to create open banking. Rather than commending the CFPB for championing the "future of banking," it's worth taking a moment to appreciate the system that already exists in the U.S., and what's at risk by virtue of the CFPB's rule.

Appendix A: Open Banking - A Global Comparison of the U.S. vs. International Models

The table below identifies core distinctions between the United States' approach under the CFPB Section 1033 rulemaking, and three of the world's most mature open banking models: Australia, the European Union and the United Kingdom.

Authority and Applicability Legal Authority

Criteria	United States	Australia	Europe	United Kingdom
Legal Authority	Dodd-Frank Act Section 1033 (Personal Financial Data Rights)	Consumer Data Right Act (Amendments to the Competition and Consumer Act 2010 and the Privacy Act 1988)	PSD2 (Directive, Not Regulation); National Competent Authorities in Each E.U. Jurisdiction; Financial Data Access Regulation (FiDA)	Payment Services Regulations (2017) Retail Banking Market Investigation Order (2017)
Primary Regulator	CFPB; The prudential bank regulators also oversee risk management for banks, despite the Dodd-Frank Act giving the CFPB exclusive authority over federal consumer financial law.	Office of the Australian Information Commissioner (OAIC); Australian Competition and Consumer Commission (ACCC)	European Banking Authority; National Competent Authorities in Member Country Jurisdictions	Financial Conduct Authority; Competition and Markets Authority

Principle #1: Data Standardization

Criteria	United States	Australia	Europe	United Kingdom
Universal Technical Standard-Setting Body	No. Individual standard-setting bodies may request CFPB recognition. Recognition	Yes. Consumer Data Standards (Formerly Data Standards Board (DSB)).	No. The PSD2 Regulatory Technical Standards (RTS) outline core principles, but there are different	Yes. Open Banking Implementation Entity (OBIE). Housed in an independent company

Criteria	United States	Australia	Europe	United Kingdom
	will last up to five years, absent revocation.		standards across E.U. member states generally established by the government (e.g., XS2A [Germany]; STET [France]).	(Open Banking Limited) funded by the nine largest U.K. banks.
Requires Data Recipients (i.e., Fintechs) to Reciprocate Data Sharing with Banks	Partially. Digital wallet providers are in scope.	Yes.	Yes.	No.

Principle #2: Consumer Safety, Consent and Disclosure

Criteria	United States	Australia	Europe	United Kingdom
Prohibits Screen Scraping	No.	No.	Significant steps to ban screen scraping. Fintech can't access bank systems to scrape their data under the guise that they are the consumer – they have to identify themselves as a third-party. A fintech also can't screen scrape if an API is available.	Significant steps to ban screen scraping. Fintech can't access bank systems to scrape their data under the guise that they are the consumer – they have to identify themselves as a third-party. A fintech also can't screen scrape if an API is available.
Requires Fintechs to Register and Obtain Accreditation	No. Any fintech can request data from a bank if the consumer authorizes the request. There are few safeguards in place to	Yes. Fintechs must meet strict technical and safety standards.	Yes. Fintechs must meet strict technical and safety standards.	Yes. Fintechs must meet strict technical and safety standards.

Criteria	United States	Australia	Europe	United Kingdom
	prevent an unsafe fintech from participating.			
Regulations Differentiate Banks from Nonbanks	Yes. Section 1033 fails to distinguish the risk between data aggregators and other third parties, such as payment initiation service providers. The regulation treats all data recipients equally, regardless of their risk level.	No. Distinguishes between accredited action initiators (AAI) who receive action requests from consumers; and Action service providers (ASP) who will perform the action request from an AAI as if it came from the consumer directly.	No. Distinguishes between account-servicing payment service providers (ASPSs), payment initiation service providers (PISPs), account information service providers (AISPs) and Financial Information Service Providers (FISP).	No. Distinguishes Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs).
Regulators Take Responsibility to Supervise and Examine Fintechs	Generally, No. Section 1033 does not include any provision for direct supervision of data recipients. In certain circumstances, the CFPB may rely on other supervisory authority.	Yes. An accredited data recipient must adhere to legal obligations and IT requirements. Data recipients must comply with ongoing obligations under the CDR Rules. The ACCC and OAIC jointly monitor compliance and enforcement.	Yes. The payment service provider will have to carry out an assessment of the operational and security risks at stake and the measures taken on a yearly basis.	Yes. Fintechs are overseen directly by the FCA.
Clear Liability Apportionment Between Data Provider and Data Recipient	No. Data providers continue to bear all liability for data breaches or fraud that	Yes.	Yes. Data holders and recipients agree on contractual liability. Payment providers are also required to obtain	Yes. Payment providers are also required to obtain minimum insurance to cover losses.

Criteria	United States	Australia	Europe	United Kingdom
	occur in providing the required data.		minimum insurance to cover losses.	

Principle #3: Data Access, Use and Retention Restrictions

Criteria	United States	Australia	Europe	United Kingdom
Requires Banks to Share Sensitive Payment Initiation Data (e.g., Account and Routing Numbers)	Yes.	Yes.	Yes.	Yes.
Allows Banks to Deny Access to Unsafe Third Parties	Unclear.	Yes.	Yes.	Yes.
Secondary Use Limitations/Data Minimization Requirements	Yes.	Yes.	Yes.	Yes.