The State of U.S. Open Banking Regulation in 2025[1]

Adam Maarec

Adam Maarec is a partner in the financial institutions compliance group at McGlinchey Stafford. He currently serves as Vice-Chair of the American Bar Association Consumer Financial Services Electronic Financial Services Subcommittee.

I. The Tech Transformation Coming for Consumer Finance: From Weekly TV Guides and Antennas to Ultra-High-Definition Streaming

Adam Maarec

It was not long ago that we would wait to get a TV Guide in the Sunday newspaper to learn which TV shows were on when. In my house, we would rush home to catch our favorite show, adjusting the antenna to get a grainy but sufficient picture of Saturday Night Live. Fast forward your VCR to today and you will find the latest shows and movies available on demand with a few clicks, in ultra-high-definition resolution. It is instant and each image contains millions of pixels, a reflection of the advances in our data processing and transmission technology. In many ways, consumer finance still relies on data as archaic as TV Guides and standard definition images, but that is changing as open banking ushers in a new era of access to real-time, high-fidelity account data.

So what is open banking, exactly? While there are a few varied definitions, open banking generally refers to the ability of consumers to grant third parties access to their bank account data. Open banking has come about in an age of changing norms and expectations regarding consumers' rights to know and control how their data is collected, used, and sold. The European Union's General Data Protection Right and California's Consumer Privacy Rights Act apply these concepts broadly across multiple sectors of the economy, with some exceptions for consumer financial data.[2] Recognizing that sensitive consumer financial data is worthy of special treatment, governments around the world have applied these principles to

1. This paper was first prepared in connection with a panel, titled *New CFPB Rules on Personal Financial Data Rights—Exploring their Impact on the Next Wave of Digital Banking*, held at the American Bar Association Business Law Section Spring Meeting in New Orleans, April 2025.
2. Ben Wolford, What is GDPR, the EU's new data protection law?, https://gdpr.eu/what-is-gdpr/; Office of Attorney Gen., Bob Bonta, California Consumer Protection Act (CCPA) (Mar. 13, 2024), https://oag.ca.gov/privacy/ccpa.

banking data and created unique open banking frameworks, with the most notable and mature being in the United Kingdom, the European Union, Singapore, and Australia.

In the United States, one of the most active open banking markets in the world has organically developed over the last twenty years without significant regulatory intervention. However, in the Fall of 2024, after an eight-year rulemaking journey, the Consumer Financial Protection Bureau ("CFPB") issued rules to govern the consumer-authorized sharing of certain banking data.[3] These rules have the potential to substantially alter the course of open banking and transform consumer finance more broadly in the years ahead.

II. Open Banking: Magnifying the Power of Consumer Financial Data

The power of data in consumer finance is unquestionable. Take credit underwriting as a key example. Traditional consumer reports are based upon data "furnished" at the end of each month by creditors, including when a consumer has applied for credit, whether credit has been granted and in what amount, and whether the consumer has paid on time or paid late throughout the life of a loan. This information is assembled and evaluated by consumer reporting agencies to create a credit score—a key measure of a consumer's creditworthiness relied on to some degree by nearly every consumer lender today. Yet, the data upon which credit reports depend has several limitations, most notably that it only includes information from creditors that choose to furnish data and that the information reported is often stale by the time it is used. For example, a missed or late payment might not be furnished by a lender to a consumer reporting agency for thirty to sixty days, or not at all.

With open banking, credit underwriting models can incorporate detailed transaction data directly from a deposit account, providing a much more granular and current view of a consumer's financial health. For example, bank account transaction details can be reviewed to determine or estimate a consumer's income, housing expenses (including mortgage payments that ordinarily appear on credit reports and rental payments that do not), and spending patterns that bear on the consumer's ability or likelihood to repay credit, such as their balances over time and whether the account has been overdrawn in the past. Credit underwriting is a key use case for detailed transaction data, but many more are emerging.

A. A Market-Led Beginning in the United States.

While regulations governing open banking are new in the United States, consumer-authorized data sharing has been active for many years. It began

3. *See* Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90838 (Nov. 18, 2024) (codified at 12 C.F.R. pt. 1001 and 1033).

with a process called screen scraping. Screen scraping is when a company seeking data collects the consumer's online banking credentials (i.e., username and password) from the consumer and stores that information. The company then uses those credentials to login to the bank's website or mobile app *as the consumer* to access the consumer's accounts and extract the desired data. The initial use case for screen scraping was to provide consumers (or their wealth managers) with a consolidated view of their finances. Instead of being required to login to multiple financial institutions for a regular update (e.g., unique sites for your credit card, mortgage, auto loan, student loan, deposits, investments, and other accounts), the company could use the consumer's credentials at multiple financial institutions to programmatically login on the consumer's behalf using its computer systems, gather the consumer's detailed account balances and transaction data, and present a consolidated view of the data from multiple financial institutions back to the consumer. Companies began gathering this data and providing insights, like helping consumers view their net worth, categorize transactions, set budgets, and get alerts based on their activity in what are generally referred to as personal financial management ("PFM") services. Companies also began accessing bank account numbers and routing numbers to initiate Automated Clearing House ("ACH") payments[4] and, in some cases, relying on the consumers' ability to login with their bank as an assurance of identity verification.

As more companies sought access to consumers' financial data, "data aggregators" stood up as service providers to satiate the demand for data and perform the laborious task of screen scraping thousands of financial institution websites, primarily on behalf of non-bank financial technology companies ("fintechs") providing innovative services that leveraged this data. As the demand for consumer financial data grew, the volume of screen scraping activities grew, which presented new risks to consumers and the financial institutions whose sites were being scraped. In the context of consumer-authorized data access, screen scraping gives the third party the ability to do everything the consumer can do online, including initiating payments or transfers and changing personal information. While risks arise when consumers grant a third party *read-only* access to their account data, accessing data via screen scraping inherently gives the third party both *read and write* access, presenting additional risks for consumers if unauthorized actions are taken. In addition, the storage of a consumer's login credentials with a third party itself creates a security risk, as a company storing many customers' passwords becomes a rich target for hackers, and the exfiltration of credential data can cause real harm if customers' accounts are accessed fraudulently.

While financial institutions began seeing increased use of their websites and mobile apps by consumers, they were inundated with logins on those

4. The ACH Network, governed by Nacha, enables payments for all U.S. bank and credit union accounts. *See* www.nacha.org.

same platforms by data aggregators seeking to screen scrape data. Financial institutions faced the difficult task of attempting to decipher which login requests on their websites were from real customers that should be admitted versus fraudsters and other risky third parties that should be blocked, all without disrupting the consumer experience. Many banks being screen scraped were also forced to grapple with the application of prudential third-party risk management obligations to these activities, which required them to manage the risks presented by all third parties, including data aggregators that were not hired by the bank.[5] Since data aggregators and other third parties accessing data are not always subject to the same regulatory data security obligations as banks, their access to sensitive financial data and bank systems presented risks that demanded attention.

B. Blocking Screen Scraping and Incentives to Migrate to APIs.

To better manage these risks, many financial institutions sought to block screen scraping activity using cyber defenses, an imperfect and challenging game of cat and mouse. These actions blocked third parties from accessing data, after which those third parties could quickly retool to get around the financial institution's defenses and continue accessing data. At the same time, data aggregators and companies seeking data sought a better way too, finding the cat and mouse game disruptive and screen scraping itself laborious and inefficient. This led large data aggregators to begin negotiating bilateral agreements with their largest targets—the country's largest banks—for access to data using more secure, sanctioned channels. This generally took the form of application programming interfaces ("APIs"). APIs are protocols used for two computers to communicate with each other in the same language. API specifications, written by the developer of the API (banks in this case), set forth instructions to access and interpret the data, i.e., the dictionary and grammar that allow the parties to communicate and understand the language.

By providing access to data via an API, banks are also able to require the consumer authenticate directly with the bank and meet their multifactor authentication requirements, i.e., require the customer to log in on the bank's website using a secret username and password, verify ownership of a device by sending a one-time PIN, verify biometrics, and pass other forms of multifactor authentication.[6] APIs also enable consumers to direct

5. *See* Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29 (rescinded with the issuance of the Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37920 (June 9, 2023)); *see also FFIEC Issues Guidance on Authentication and Access to Financial Institution Services and Systems*, Fed. Fin. Inst. Examination Council (Aug. 11, 2021), https://www.ffiec.gov/news/press-releases/2021/pr-08-11.

6. This is generally referred to as the OAuth protocol, an open-source technology specification for third party data access that is used in many applications today. *See OAuth 2.0*, OAuth, https://oauth.net/2/ (last accessed Jan. 6,

their bank to share data with a specific third party—a requirement for the sharing of "nonpublic personal information" with unaffiliated third parties under the Gramm-Leach-Bliley Act ("GLBA").[7] This process then allows banks to provide consumers with access controls, creating a valve for consumers to shut off the flow of data out of the bank *directly with the bank.* APIs also provided benefits to data recipients, primarily by eliminating the need for resource-intensive screen scraping, ensuring consistent access without disruptions, and obtaining data with a higher level of accuracy.

C. Standardizing Data: the Financial Data Exchange.

Each bank's API amounts to their own bespoke language for users of the API to learn. For third parties seeking access to data via API across thousands of banks in the United States, having so many bespoke languages to learn makes integrating with multiple banks inefficient and limits the interoperability of their datasets. These challenges led to the need for standardized APIs, where banks and other companies could communicate data using a single language. So, multiple banks, data aggregators, and fintechs came together to create the Financial Data Exchange ("FDX") with the objective of creating a ubiquitous, royalty-free API specification.[8] In other words, FDX's founders set out to create a single language, dictionary, and series of communication rules to enable the interoperability of financial data across financial institutions and fintechs.

At the same time, data aggregators became linguistic masters, learning to interpret, normalize, and clean data from multiple financial institutions—gathered via both APIs and screen scraping—and then selling that data to companies in yet another language, i.e., the data aggregator's pro-

2025). OAuth generally allows a company seeking access to data to: (a) authenticate with the data provider (e.g., a bank); (b) redirect the consumer to the data provider to authenticate or login, and pass other steps the data provider requires, such as obtaining an express authorization to share data within defined parameters (e.g., what data and for how long); and (c) obtain a secret code from the data provider that can then be presented later to access the data that has been authorized for sharing.

7. *See* 12 C.F.R. § 1016.15(a)(1) (permitting disclosure of "nonpublic personal information," without regard to consumer opt-out choices and other requirements, if the disclosure is with "the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction").

8. *See* www.financialdataexchange.org ("FDX is a non-profit industry standards body operating in the US and Canada that is dedicated to unifying the financial services ecosystem around a common, interoperable and royalty-free technical standard for user-permissioned financial data sharing, aptly named the FDX API. . . . FDX is committed to five core principles of financial data sharing to empower end users to better understand, leverage, and benefit from their own financial data in a secure and reliable manner. These principles are: Control, Access, Transparency, Traceability and Security.") (last accessed Jan. 19, 2025).

prietary API format. Companies wanting to access and use consumer financial data often do not have the expertise or resources to integrate with many bank APIs, let alone engage in screen scraping, so contracting with a single data aggregator to obtain all of that data in a single normalized dataset is a valuable service for a company. But once a third party begins to ingest data from one data aggregator using the data aggregator's proprietary API, it becomes harder to move to a new data aggregator because of the need to integrate with the new data aggregator's APIs and data formats, to essentially learn a new language. I discuss the challenges with interoperability in more detail below.

III. A New Regulatory Regime Takes Shape

In the aftermath of the 2008 financial crisis, the U.S. Congress passed the Dodd–Frank Wall Street Reform and Consumer Protection Act ("the Dodd–Frank Act"), which included provisions to create the CFPB. Section 1033 of the Dodd-Frank Act was a relatively short and largely uncontroversial provision of the law granting consumers the right to receive information about their financial products or services electronically upon request. It also gives the CFPB authority to write implementing rules. The operative language states that:

> *Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.*[9]

Untouched for six years, it was not until 2016 that the CFPB turned its attention to the growing ecosystem surrounding consumer-authorized data sharing and issued a *Request for Information Regarding Consumer Access to Financial Records*.[10] Following the receipt of comments from the public, the CFPB issued non-binding *Principles For Consumer-Authorized Financial Data Sharing and Aggregation* in the fall of 2017.[11]

The CFPB's principles included high-level expectations for consumer-authorized data sharing, including ensuring that:

- Consumers could access a certain scope of current, accurate, and usable data;

9. 12 U.S.C. § 5533(a).
10. *See* Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83806 (Nov. 22, 2016).
11. *See Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, Consumer Fin. Prot. Bureau (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

- Consumers would be provided with meaningful disclosures, provide informed consent to access data, and have control over ongoing access with a certain level of transparency, e.g., to know who is collecting what data and when;
- Payment authorizations were treated distinctly from data sharing authorizations; and
- Minimum security standards were applied, that consumers could dispute and resolve instances of unauthorized access, and effective accountability existed if risks, harms and costs were imposed on consumers.

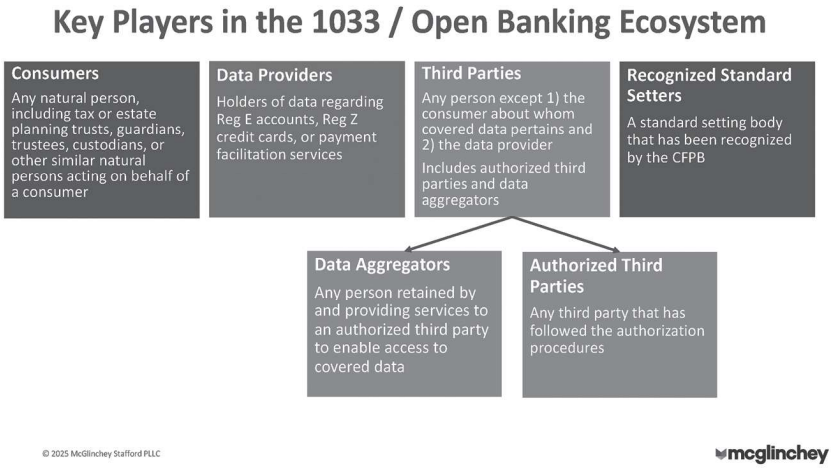
The CFPB began its current rulemaking process in earnest in October 2022 by releasing an outline of what it rebranded as rules governing "Personal Financial Data Rights" for feedback from small businesses.[12] Since the outline impacted the entire data sharing ecosystem, many others took the opportunity to comment on the outline as well, including larger entities, academics, and consumer advocates. The agency then issued a report summarizing the feedback it received in March 2023,[13] followed by an Advanced Notice of Proposed Rulemaking in October 2023.[14] After receiving public comments, the CFPB finalized its rules in two phases, first issuing final rules regarding Industry Standard Setting in June 2024[15] and a complete final rule on Personal Financial Data Rights in November 2024.[16]

This paper does not explore the nuances of how the final rules changed over the course of this two-year process because, in part, the changes were not that substantial. Instead, the next section explores the parts of the final rules that are largely agreed upon by industry participants, the parts of the final rules where substantial controversy or ambiguity remains, and concludes with thoughts on the practical path forward for data providers and third parties.

12. *See* Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights, Consumer Fin. Prot. Bureau (Oct. 27, 2022), https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.
13. *See Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Required Rulemaking on Personal Financial Data Rights*, Consumer Fin. Prot. Bureau (Mar. 30, 2023), https://files.consumerfinance.gov/f/documents/cfpb_1033-data-rights-rule-sbrefa-panel-report_2023-03.pdf.
14. *See* Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796 (Oct. 31, 2023) (codified at 12 C.F.R. pt. 1001 and 1033).
15. *See* Required Rulemaking on Personal Financial Data Rights; Industry Standard-Setting, 89 Fed. Reg. 49084 (June 11, 2024) (codified at 12 C.F.R. pt. 1033).
16. *See* Required Rulemaking on Personal Financial Data Rights, *supra* note 3.

IV. New Rules of the Road: An Overview of the CFPB's Final Rules on Personal Financial Data Rights

The CFPB's final rules governing Personal Financial Data Rights identify the following key players in the open banking ecosystem:



At its core, the rule requires data providers to make available to consumers and authorized third parties, upon request, the most recently updated and historical covered data in their control or possession.[17] To do this, data providers must:

- Maintain a "*consumer interface*" to receive requests and make covered data available in an electronic form *usable by consumers*, e.g., a bank's website and mobile app; and
- Maintain a "*developer interface*" to receive requests and make covered data available in a standardized and machine-readable format *usable by authorized third parties*, e.g., a bank's API.[18]

Also central to the rule is the creation of a new *right for authorized third parties to access covered data*.[19] To become an authorized third party with that right, a third party must:

- Seek access to covered data from a data provider on behalf of a consumer to provide a requested product or service;
- Provide the consumer with an "authorization disclosure" including a statement certifying the third party's commitment to follow all applicable 1033 obligations; and

17. *See* 12 C.F.R. 1033.201.
18. *See* 12 C.F.R. 1033.301.
19. *See* 12 C.F.R. 1333 Subpart D.

- Obtain the consumer's express informed consent via a signed authorization disclosure.[20]

V. Uncontroversial Issues in the Final Rule

A. Consumer-facing Disclosures.

Authorized third parties must provide consumers with clear disclosures regarding the scope of data to be accessed, the parties that will have access to data, the duration of access, and revocation instructions. Data providers also have a right to confirm certain aspects of the authorization with the consumer, including the accounts and data that may be accessed. These disclosures are generally viewed positively and without controversy, though some would have liked to see model disclosures.

B. Data Security Requirements for All.

As a condition to becoming an authorized third party, an entity is required to apply the GLBA's Safeguards Rules to its collection, use, and retention of data, following either the prudential banking regulators' rules or the Federal Trade Commission's ("FTC") rules, as the case may be.[21] While the prudential banking regulators' version of the GLBA Safeguards rule is different than the FTC's version of the rule, the differences were narrowed when the FTC enhanced its requirements for non-banks in 2021 amendments to its rules.[22] Differences in these Safeguards Rules still remain, but they are less significant now than in the past. In addition, the lack of formal federal supervision over non-bank entities' implementation of these data security requirements continues to be a concern for financial institutions.

20. *See* 12 C.F.R. 1033.401.

21. *See* 12 C.F.R. § 1033.421(e). The GLBA provides multiple regulatory agencies rule writing authority with respect to data security. Section 1033.421(e) applies either the data security requirements of Section 501 of GLBA for authorized third parties that are financial institutions subject to GLBA, or the FTC's Standards for Safeguarding Customer Information, 16 C.F.R. pt. 314, for other authorized third parties. Section 501 is implemented in the Interagency Guidelines Establishing Standards for Safety and Soundness, 12 C.F.R. pt. 30, app. A (OCC); 12 C.F.R. pt. 208, app. D-1 (Bd. of Governors of the Fed. Rsrv. Sys.); 12 C.F.R. pt. 364, app. A (FDIC); 12 C.F.R. pt. 748, app. A (NCUA)).

22. *See* Standards for Safeguarding Customer Information, 86 Fed. Reg. 70272 (Dec. 9, 2021) (codified at 16 C.F.R. pt. 314) (revising the agency's Standards for Safeguarding Customer Information to: provide more guidance on how to develop and implement an information security program, such as access controls, authentication, and encryption; requiring periodic reports to boards of directors or governing bodies; expanding the definition of "financial institution" to include activities of "finders," among other things).

VI. Areas of Controversy and Ambiguity in the Final Rule

A. Data Access, Use & Retention Limitations.

Any access, use, or retention of data by an authorized third party must be limited to what is "reasonably necessary" to deliver the requested product or service. This approach to data governance is wholly new in federal consumer financial services law. GLBA provides a notice and opt-out regime to permissible data sharing,[23] and the Fair Credit Reporting Act ("FCRA") places limits on the "permissible purposes" for which consumer report information can be used,[24] but neither uses the "reasonably necessary" standard found in the final 1033 rule.

So, regardless of what terms of use appear in a third party's terms and conditions or privacy policies, secondary uses of data beyond what's reasonably necessary to deliver the requested product or service are generally prohibited. In this way, the final 1033 rule places additional restrictions on the access, use, and retention of financial data above and beyond the restrictions that already exist—and continue to apply—under GLBA and FCRA. The final rule states that it is almost always not reasonably necessary and thus an improper secondary use of data to engage in targeted advertising, to cross-sell other products or services, or to sell data to third parties.[25]

While data providers may applaud the restrictions on downstream uses of data—such as to the use of data to build unrelated models or reverse-engineer confidential or proprietary algorithms—recipients of data seeking to use it for innovative use cases may find themselves constrained and struggle to determine and operationalize controls to ensure their access, use, and retention of data is appropriately limited. In practice, this requires every use of data to be evaluated against the original reason for which it was collected. Moreover, the obligation to retain data only as long as reasonably necessary amounts to an obligation to purge data once retention is no longer necessary or justifiable, which also presents operational challenges.

B. Scope of Covered Data is Narrow and Imprecise.

The scope of data covered by the final rule is limited to "covered data" regarding certain accounts, namely credit cards under Regulation Z[26] and accounts under Regulation E (e.g., deposit accounts and prepaid cards),[27]

23. *See* 15 U.S.C. § 6802.
24. *See id.* § 1681b.
25. *See* 12 C.F.R. 1033.421(a).
26. *See* 12 C.F.R. § 1026.2(a)(15)(i) (defining a "credit card" as "any card, plate, or other single credit device that may be used from time to time to obtain credit" and including a hybrid prepaid-credit card).
27. *See id.* § 1005.2(b) (defining an "account" to include a "demand deposit (checking), savings, or other consumer asset account . . . held directly or indirectly by a financial institution and established primarily for personal, family,

and payment facilitation services. However, Section 1033 of the Dodd-Frank Act provides data access rights for *all* consumer financial products and services. The CFPB was purposeful in defining the scope of the final rule this way, exempting and leaving many products out of scope, including mortgages, auto loans, and student loans.[28] The CFPB's rationale is that Regulation E accounts and credit cards are consumers' primary transaction accounts with the most valuable data, including data that reflect payment activity on other debts, e.g., mortgage and auto loan payments debited from a deposit account will be visible to an authorized third party under the final rule even though mortgage and auto loan accounts are not in scope. The CFPB also referenced that it may conduct future rulemakings to cover more products, including government benefits (also referred to as electronic benefit transfer or EBT cards).[29] Notwithstanding the narrow scope of the final rule, demand for access to data from other types of accounts is likely to continue, from additional types of consumer debt and asset accounts to payroll, investments, pensions, insurance, small business accounts, and other products and services.

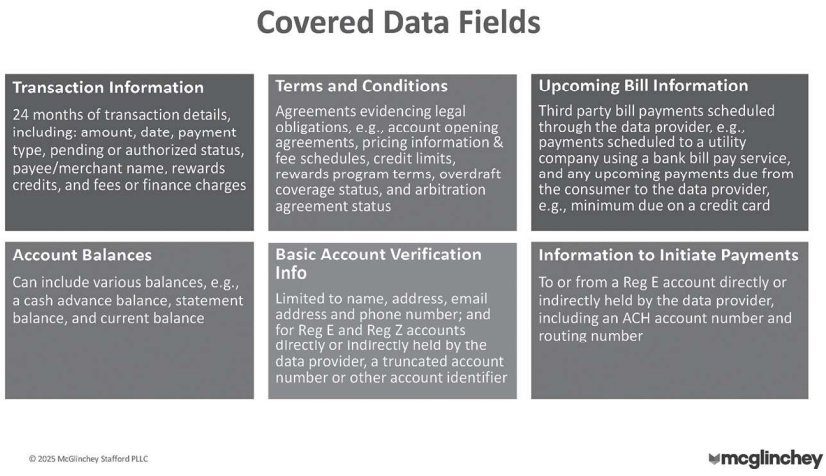
The final rules identify six broad categories of data that must be available—transaction information, terms and conditions, upcoming bill information, account balances, basic account verification information, and information to initiate payments—along with a few examples of each. However, the examples are not exclusive, and the data within each category is subject to interpretation. A series of exceptions also apply, permitting data providers to avoid sharing confidential commercial information, information collected solely to prevent fraud or money laundering, infor-

or household purposes" and a prepaid account). The CFPB recently proposed an interpretive rule expressing an expanded view of the types of services that are covered as "other consumer asset accounts," concluding that "Depending on the facts and circumstances, the following could be considered 'accounts' under EFTA: video game accounts used to purchase virtual items from multiple game developers or players; virtual currency wallets that can be used to buy goods and services or make person-to-person transfers; and credit card rewards points accounts that allow consumers to buy points that can be used to purchase goods from multiple merchants." Electronic Fund Transfers Through Accounts Established Primarily for Personal, Family, or Household Purposes Using Emerging Payment Mechanisms, 90 Fed Reg. 3723 (Jan. 15, 2025) (codified at 12 C.F.R. pt. 1005). Note that the interpretive rule was withdrawn by the CFPB "because further rulemaking action with respect to this proposal does not align with current agency needs, priorities, or objectives." *See* 90 Fed. Reg. 20568 (May 15, 2025). The withdrawal notes that "comments received . . . raise multiple issues warranting further attention related to, for example, whether the proposed interpretive rule properly interprets the EFTA."

28. *See* Required Rulemaking on Personal Financial Data Rights, *supra* note 3 at 90853-90856.

29. *Id*. at 90856 (stating that "The CFPB intends to implement CFPA section 1033 with respect to other covered persons and consumer financial products or services through future rulemaking").

mation required to be kept confidential by law, and information that the data provider cannot retrieve in the ordinary course of business.[30] Data providers must examine and document the data they have, the data they will choose to make available, and the data they will choose to not make available, and why.



C. Payment Initiation Competition and the Potential for Increased Fraud.

The sharing of payment initiation information, namely account numbers and routing numbers that can be used to initiate an ACH transfer, presents an opportunity for "pay by bank" services to grow and compete with the existing credit card and debit card payment networks.[31] Coupling payment initiation with data from the related bank account allows pay by bank services to initiate ACH payments with enhanced risk management capabilities. For example, each ACH payment can be given a risk score the moment it is initiated based on the account's current balance information, scheduled bill payments, and transaction history, among other data elements. The risk score helps predict the likelihood of the payment successfully being cleared and accepted by the customer. The CFPB's emphasis on

30. *See* 12 C.F.R. 1033.221.

31. "Pay by bank" services generally refer to electronic checkout solutions that allow a consumer to pay using their online banking credentials rather than a credit card or debit card. In a typical e-commerce transaction, rather than entering a credit card or debit card number at checkout: the consumer is redirected from a merchant website, in many cases by a data aggregator, to login with their bank; the consumer directs the bank to share their bank account number and routing number with the merchant; and the merchant uses the consumer's bank account number and routing number to initiate an ACH payment.

enhancing competition in payments, and leaning on open banking as a means to enhance competition with the existing payment networks, is consistent with the concerns raised by the Department of Justice when it sued to block the acquisition of a large data aggregator by a large payment network.[32]

At the same time, financial institutions that provide consumer accounts subject to Regulation E are concerned that providing payment initiation information to a broad swath of third parties will result in increased fraud without appropriately allocated liability. They argue that the ACH network, unlike the credit card networks, such as Visa and Mastercard, is not built to manage a high volume of point of sale transactions and does not have the operational infrastructure or governance mechanisms needed to manage a high volume of disputes. Moreover, the CFPB noted in the final rule that Regulation E's consumer protections continue to apply to these transactions.[33]

To assuage these concerns, the final rules permit tokenized account numbers ("TANs") to be shared in lieu of an account number. TANs are secondary account numbers for a bank account that allow its provider to implement controls and better assess each payment using the TAN.[34] For example, if a TAN is provided to Merchant A, the use of that TAN by Merchant B would represent a higher risk than a payment initiated by Merchant A, the intended recipient and user of the TAN, and the issuer of the TAN could choose to decline transactions using the TAN by Merchant B. However, the final rule notes that TANs may not be used as a "pretext to restrict competitive use" of the account number or payment rail, leaving in question which types of fraud prevention parameters can be placed on TANs and account numbers accessed via 1033 more broadly.[35] Given the CFPB's recent focus on the need for adequate fraud prevention mechanisms to be implemented by financial institutions in connection with digital payment services,[36] the need to manage potential fraud from pay by bank services is acute.

D. No Ban on Screen Scraping.

While the final rule criticizes screen scraping as an inherently risky practice, it does not prohibit third parties from screen scraping. In perhaps the

32. *See* U.S. Dep't of Just., Press Release, *Justice Department Sues to Block Visa's Proposed Acquisition of Plaid* (Nov. 5, 2020), https://www.justice.gov/opa/pr/justice-department-sues-block-visas-proposed-acquisition-plaid.
33. For example, the provisions regarding consumer liability for unauthorized transfers and procedures for resolving errors. *See* 12 C.F.R. pt. 1005.6; 1005.11.
34. *See* 12 C.F.R. 211(c).
35. *See* 12 C.F.R. 211(c)(1).
36. *See CFPB Sues JPMorgan Chase, Bank of America, and Wells Fargo for Allowing Fraud to Fester on Zelle*, Consumer Fin. Prot. Bureau (Dec. 20, 2024), https://www.consumerfinance.gov/about-us/newsroom/cfpb-sues-jpmorgan-chase-bank-of-america-and-wells-fargo-for-allowing-fraud-to-fester-on-zelle/.

most backwards aspect of the final rule, the CFPB states that *data providers* may not rely on screen scraping to make covered data available to third parties and must instead create compliant developer interfaces (i.e., APIs). This is backwards because third parties, primarily data aggregators, are the companies that initiate and rely on screen scraping to access data, and data providers are forced to manage the ramifications of those activities.[37] In this regard, the burden of ending screen scraping is shifted by the final rule to data providers instead of the companies that initiate screen scraping. Additionally, while data providers are not obligated to block screen scraping, they likely have the right to block screen scraping if specific risks can be identified.[38]

But the challenges don't stop there. Data providers that create fully compliant developer interfaces must still grapple with the fact that third parties may demand access to data that is not currently "covered data"—including data about Regulation E accounts and Regulation Z credit cards that are out of scope, and data about other out of scope products like mortgages, auto loans, and student loans—and that third parties may seek that data via screen scraping. The CFPB noted in the final rule that a data provider's effort to block access to such data could be considered an unfair, deceptive, or abusive act or practice, leaving them without any good options.[39]

E. The Third Party Risk Management Bottleneck.

Banks have third party risk management obligations based on prudential safety and soundness requirements.[40] When acting as a data provider, the final 1033 rules generally permit reasonable denials of access to data (via the developer and consumer interfaces) if the denial is necessary to comply with prudential safety and soundness standards, GLBA Safeguards, or other laws and regulations regarding risk management.[41] A denial is considered reasonable if directly related to a specific risk of which the data provider is aware (e.g., data security practices), and the denial is applied consistently and in a non-discriminatory manner. Additional "in-

37. In one high profile lawsuit involving screen scraping of bank data, a bank sued to stop a data aggregator from using their logo when initiating screen scraping. *See PNC Sues Plaid Over Alleged Trademark Infringement*, PYMNTS (Dec. 23, 2020), https://www.pymnts.com/legal/2020/pnc-sues-plaid-over-alleged-trademark-infringement/.
38. *See* Required Rulemaking on Personal Financial Data Rights, *supra* note 3 at 90895.
39. *Id*.
40. *See* Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37920 (June 9, 2023). Note that these standards are issued and implemented by three different federal regulators: The Board of Governors of the Federal Reserve System, the FDIC, and the OCC. While these regulators are generally aligned in their approach to third party risk management, their priorities and focus may differ in practice.
41. *See* 12 C.F.R. 1033.321.

dicia of reasonableness" of a denial include adherence to a consensus standard on risk management, whether the denial is based on standardized risk management criteria made available to the third party, and whether the third party has a "certification or other identification of fitness to access covered data" from a recognized standard setter or the CFPB.[42]

In practice, data providers will need to create sophisticated third party risk management protocols to evaluate an expected influx of requests to access data from third parties initial access requests and ongoing access requests and ensure the criteria and process is applied evenly to all third parties seeking access to covered data. At least three key issues remain when data providers consider whether to grant a third party access:

— Evaluation of "fourth parties." What third party risk management criteria should data providers apply to each authorized third party accessing data via a data aggregator, if any? For example, if a data provider evaluates and grants access to a data aggregator that has met their third party risk management expectations, what amount of risk management must be applied to each of the data aggregator's clients seeking access to data (each would be an authorized third party under 1033 and a fourth party to the data provider)?

— Role of standards and certifications. There is not a ubiquitous 1033 data access risk management standard today. On one hand, the development of a consensus standard on risk management will be instrumental in standardizing efficient third party risk management reviews. On the other hand, the objective of standardization is at odds with overarching view of prudential third party risk management requirements as varying based on the specific facts and circumstances presented and each bank's individual risk profile.[43] Any

42. *See* 12 C.F.R. 1033.321(c).

43. *Id*. (stating that a sound bank risk management program analyzes "the risks associated with each third-party relationship and tailors risk management practices, commensurate with the banking organization's size, complexity, and risk profile and with the nature of the third-party relationship."). The Federal Deposit Insurance Corporation issued a Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services in July 2020, acknowledging the challenges that varied third party risk management expectations present to the adoption of new technology. *See* 85 Fed. Reg. 4890 (July 24, 2020). The idea was promoted recently by the FDIC Vice Chairman Travis Hill. *See also* Speech, Vice Chairman Travis Hill, Charting a New Course: Preliminary Thoughts on FDIC Policy Issues, FDIC (Jan. 10, 2025), https://www.fdic.gov/news/speeches/2025/charting-new-course-preliminary-thoughts-fdic-policy-issues ("It is also worth revisiting the possibility of a public-private standard setting organization that would establish standards for due diligence of fintech vendors and technologies, which would reduce the need for each bank that partners with a fintech to conduct costly, time-consuming due diligence of its own.").

risk management standard will need to balance the need for consistency and uniformity with the need for customization by the bank. Moreover, the degree of reliance that data providers place upon a "certification or other identification of fitness to access covered data" remains in the data providers' discretion, and none of these certifications exist today.[44]

— A looming battle on liability and bilateral agreements. The CFPB chose not to apportion liability for the various types of errors that can occur throughout and in connection with 1033 data sharing, instead deferring to liability allocation regimes under existing law. So, errors from unauthorized ACH transfers and credit card payments should be handled according to Regulation E and Regulation Z error resolution frameworks, respectively. The final rule also notes that liability arising out of privacy or other issues may be appropriately managed in bilateral agreements between a data provider and third party. With respect to bilateral agreements, the CFPB acknowledges an ongoing need for them and that data providers may need to onboard third parties in a staggered manner.[45] While the CFPB's discussion of specific terms appropriate for a bilateral agreement is limited, the agency notes that wholesale indemnification or hold harmless terms will be viewed skeptically, as will attempts to allocate losses from unauthorized transactions that arise under Regulation E or are subject to network rules that provide a better means to allocate liability than one-off agreements.[46]

---

44. *See* 12 C.F.R. 1033.321(c) and Required Rulemaking on Personal Financial Data Rights, *supra* note 3 at 90902.

45. Required Rulemaking on Personal Financial Data Rights, *supra* note 3 at 90846–47.

46. *See* Required Rulemaking on Personal Financial Data Rights, *supra* note 3 at 90900. The Clearing House Payments Company, which owns and operates core payments system infrastructure in the U.S., formed the Connected Banking Initiative "focused on accelerating the ability of data providers, (e.g. banks) and data receivers, (e.g. data aggregators or fintechs) to establish safe and secure direct connections through application programming interfaces (or APIs)." The Connected Banking Initiative observed that "legal agreements between banks and fintechs have sometimes taken 12 months or more to be developed and finalized and have become a significant bottleneck to API adoption." To alleviate that bottleneck, the Connected Banking Initiative developed "a Model Agreement that banks and data aggregators/fintechs can use as a reference to facilitate the development of API-related data sharing agreements." While drafted prior to the final rule being issued, the model agreement provides examples of key terms ordinarily included in data access agreements, including terms governing: technical integration; record retention; audits; security reviews and assessments; data safeguards and breach protocols; quality assurance and governance; personnel requirements; representations and warranties; termination and suspension; intellectual property; confidentiality; liability and

F. The Prohibition on Data Provider Fees.

The final rule prohibits data providers from charging fees for access to covered data.[47] While seemingly intended to ensure that *consumers* have free access to data, it also entitles data aggregators and authorized third parties to access data without paying the data provider any fees for their efforts to enable access. This policy places the financial burden to create more secure data sharing technology on data providers while delivering the benefits of access to standardized data to third parties, and permitting data aggregators and other third parties to charge fees for access to the same data which they obtain for free from data providers.

Data providers are concerned that, without the ability to charge some fees to recover their costs for building and maintaining services for *third parties*, there will not be any incentive for third parties to limit the volume or frequency of their data requests. Whether data providers may be able to create some permissible fee structures related to accessing data, such as fees for premium services or arranging for access to data outside the 1033 framework, is yet to be seen.

G. Looking to Standard Setters for Indicia of Compliance.

The final rule creates a process to recognize "standard setters" that will issue technical specifications for data sharing and other specific topics related to compliance with the final rule.[48] Standard setters must apply to be recognized by the CFPB and, in order to be accepted, possess several key characteristics, including: openness and transparency in their decision making processes; balance across decision makers representing a variety of interested partners; due process and measures to allow appeals; and decision making by consensus.[49] As of this writing, one standard setter has been conditionally recognized by the CFPB: the Financial Data Exchange.[50]

The standards to be issued by recognized standard setters address a number of areas, some of which are technical, such as data formats, developer interface documentation, downtime notices, and performance response times. Other standards reflect more substantive processes, including the selection of data fields to be provided, access frequency restrictions,

---

indemnification; dispute resolution; etc. The model agreement is available here: https://www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/TCH_Data_Access_Agreement_10-31-19_FINAL.pdf?rev=3e53169f55164554a61bcf7b33255db3&hash=270F9819757607FB3701C45F1328EBAF (last accessed Jan. 19, 2025).

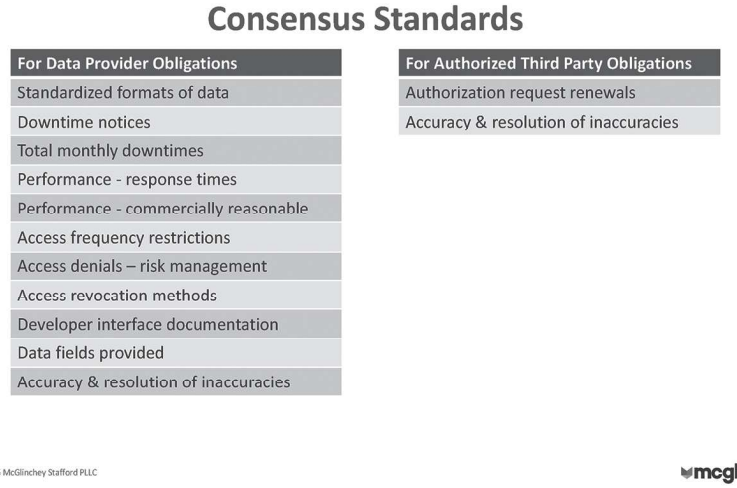
47. *See* 12 C.F.R. 1033.301(c).

48. *See* 12 C.F.R. 1033.141.

49. *Id*.

50. *See* In re Financial Data Exchange, Inc., Application for Recognition, 2024-CFPB-PFDR-0001 (Jan. 8, 2025), https://files.consumerfinance.gov/f/documents/cfpb_standard-setter-decision-and-order-of-recognition-fdx_2025-01.pdf.

access denials, processes to ensure the accuracy of data, and processes to resolve data inaccuracies. The table below describes the various areas where consensus standards may be issued and to which entity those standards would apply.



Adhering to a particular consensus standard issued by a recognized standard setter will provide the company with an "indicia of compliance" with certain sections of the rule, which falls short of a complete "safe harbor" or compliance guarantee. Nonetheless, a company that chooses not to follow a consensus standard will likely be expected to explain why it chose not to follow or to deviate from a particular standard. In some ways, following a consensus standard provides a rebuttable presumption of compliance, while not following a standard creates a rebuttable presumption of non-compliance. The ability to influence these standards will thus be of utmost importance to companies that must adhere to them.

A recognized standard setter could go further by writing standards—or other guidelines or best practices—regarding issues that are not directly addressed by the rule, though following these would not expressly serve as "indicia of compliance" with the rule.

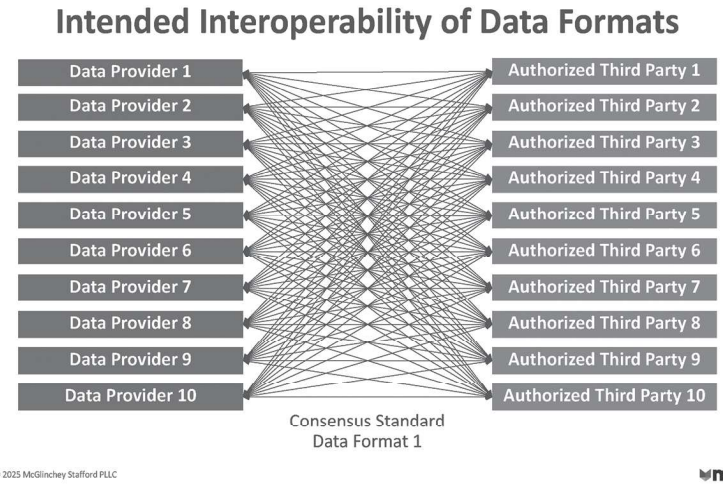
H. Interoperability Comes in Degrees.

The CFPB intends for the final 1033 rules to promote standardized and interoperable data, so that consumers can more easily export their data and switch providers. To that end, the final rules require data providers to make data available through their developer interfaces using a "standardized format," which is defined to include both the: 1) structures and definitions of covered data, i.e., a dictionary that enables data elements to be understood; and 2) protocols for communicating requests and responses for covered data, i.e., a grammar guide so that APIs can communicate data.[51]

51. *See* 12 C.F.R. 1033.311(b).

Following the analogy between APIs and language, these standardized "data format" requirements require data providers to choose a single standardized language in which to communicate financial data, publish their data dictionaries and grammar guides, and speak that language consistently via its developer interface.[52] In theory, this will allow third parties to learn a single language and access data from multiple data providers that they can understand.

The following chart depicts how, with a single consensus standard for data formats, multiple authorized third parties can connect to multiple data providers without the need for intermediaries.



But the panacea of fully interoperable data faces several practical challenges:

— Data providers may choose from multiple standards. A data format is considered "standardized" under the final rule if: 1) it is widely used by other data providers and designed to be readily usable, of which there could be several; *or* 2) it is a consensus standard issued by a recognized standard setter, of which there could be several.[53] The first option does not exist today as most data providers' APIs are custom built solutions, and the collaboration among data providers to create a new standard for themselves could invite antitrust scrutiny.[54] And even if multiple data providers choose to follow the same data formatting standard, a myriad of decisions are made by

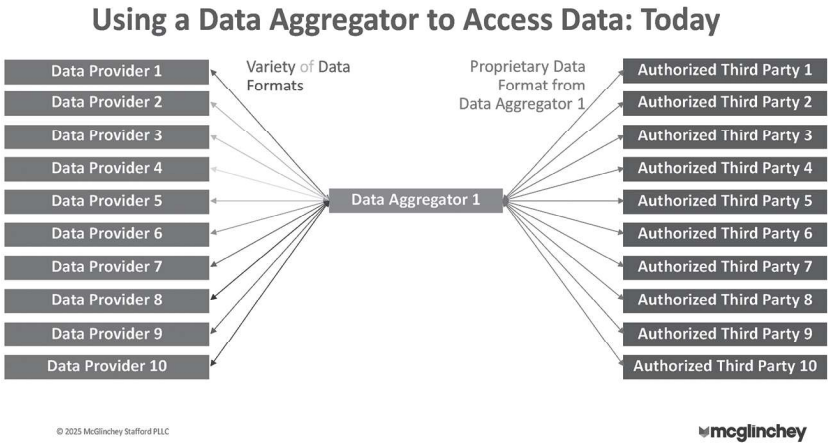
52. *Id.*
53. *Id.*
54. *See Prepared Remarks of CFPB Director Rohit Chopra at the Financial Data Exchange Global Summit*, Consumer Fin. Prot. Bureau (Mar. 13, 2024), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-at-the-financial-data-exchange-global-summit/.

a user in their implementation that could make third-party integrations challenging—for example, decisions regarding which specific data to provide, which authentication and data security protocols to use.

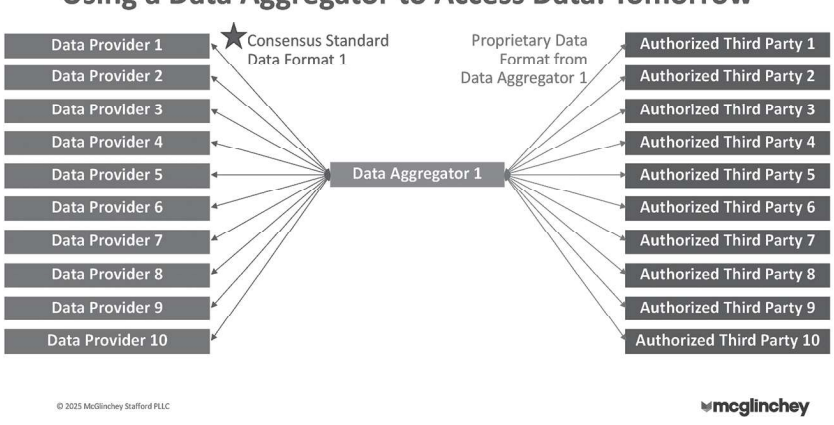
— Integrating with multiple data providers for direct access to data takes work. Even assuming that most data providers will choose to follow a single data formatting standard—the Financial Data Exchange is the most popular in the U.S. today—third parties seeking direct access to data from multiple financial institutions will face challenges.

First, third parties will likely need to enter bilateral contracts with data providers to care for safety and soundness concerns, liability allocations, and other risks not adequately addressed by the final rules, and data providers are likely to take differing positions on the risks presented and specific mitigations required. Moreover, data providers will need to build bespoke third party contracting and risk management processes for data aggregators and authorized third parties that do not fit within their existing vendor management systems, many of which will need to be refined over the coming years.

Second, integrating with multiple different APIs requires significant technical resources, such as establishing sandbox access and testing, even if the APIs are largely standardized. Ongoing technical maintenance will be needed as well. It may be worth the effort and investment for some third parties to seek direct access to covered financial data from data providers, particularly since data providers are prohibited from charging fees for access to data. In the alternative, third parties may find it easier and less expensive to hire a data aggregator to access data from data providers on their behalf. The diagram below demonstrates how a data aggregator can establish access to multiple data providers following a variety of data formats, and that authorized third parties can then obtain data from the data aggregator in a single data format. But, as discussed further below, using a data aggregator comes with its own risks and challenges, particularly when it comes to interoperability because the data is often formatted using the data aggregator's own proprietary data format.

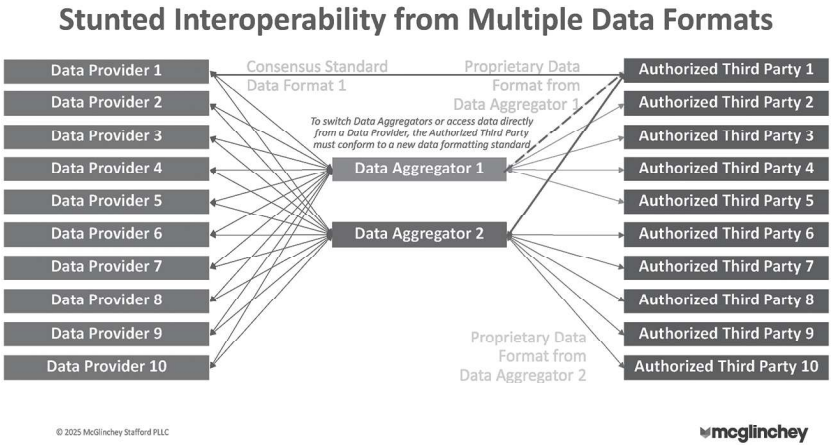


— Data aggregators are not required to use standardized data formats, eliminating the benefits of interoperability for their customers. Under 1033, only data providers are required to use standardized data formats. Data aggregators are not required to follow those same standardized data formatting requirements. In practice, this means that data aggregators will access data on behalf of authorized third parties in a standardized data format from data providers, and then share that data with authorized third parties using its own proprietary data format, as shown in the diagram below.



Data aggregators may offer good reasons to follow their format—for example, to present normalized or cleaned data from multiple providers, to incorporate new data derived from its evaluation of data—such as estimated annual income based on direct deposits or total net worth based on account balances from multiple providers—or to append data from other sources, such as consumer report data.[55]

But data aggregators that choose to only provide data using their proprietary data format limit the intended benefits of interoperability sought by the CFPB's final rules. These proprietary data formats make it difficult for authorized third parties to switch to a new source of data—whether from another data aggregator that uses its own proprietary data format or directly from data providers using standardized data formats. The graphic below illustrates how the benefits of interoperability can be stunted when multiple data formats are used.



VII. Some Headwinds for the Final Rule Won't Stop Open Banking's Momentum

The CFPB's final 1033 rules could face challenges in the months ahead. A few key areas to watch are summarized below.

55. Protecting Americans from Harmful Data Broker Practices (Regulation V), 89 Fed. Reg. 101402 (Dec. 13, 2024) (noting the CFPB proposed a rule to regulate data brokers under the FCRA stating that data aggregators that merely reformat data received from a data provider could be assembling or evaluating data and thus acting as a consumer reporting agency).

A. Banking Trade Associations' Lawsuit Challenging the Final Rule.

Two banking trade associations filed a lawsuit challenging the final rule in the Eastern District of Kentucky.[56] Their Amended Complaint includes ten claims under the Administrative Procedures Act, including claims that several aspects of the CFPB's final rule are arbitrary and capricious—the CFPB's interpretation of "consumer" to broadly include third parties, placing consumer data at risk, restricting access denials based on risk management, failing to address liability, imposing vague developer interface performance standards, setting irrational compliance deadlines, and imposing the access-fee ban—and exceed the agency's statutory authority, which requires the disclosure of payment initiation information, delegating regulatory authority to private standard setters, and imposing the access-fee ban. Some of the claims dispute the propriety of key provisions of the rule, including that the Dodd-Frank Act only requires access by the consumer and does not extend access rights to third parties, and that the CFPB cannot permit industry standard setters to set indicia of compliance. Should they prevail on the merits, certain provisions or the entire rule could be set aside, or the court could enjoin the CFPB from enforcing the rule.

B. Congressional Review Act.

Since the rule was finalized and published in the Federal Register on November 18, 2024, within sixty legislative days of the 118th Congress adjourning, it is subject to disapproval by Congress under the Congressional Review Act ("CRA").[57] A resolution of disapproval under the CRA would need to be passed by Congress and signed by the President. If that were to occur, the resolution would effectively nullify the rule *and* prohibit another rule from being issued in "substantially the same form." But a CRA resolution of disapproval seems unlikely given bipartisan support for increased data sharing and competition in the provision of banking-related services from the fintech sector.[58]

C. Changes in Leadership and Priorities at the CFPB.

New leadership at the CFPB, namely the appointment of a new Director that shares different perspectives than the prior administration that promulgated the final rules, could result in an effort to change the rule. Such changes would follow the ordinary process in the Administrative Procedures Act, including publication of a proposed rule that establishes the

56. Complaint, Forcht Bank, N.A. v. CFPB, 5:24-cv-00304-DCR (Ky. filed Nov. 18, 2024).

57. *See* 5 U.S.C. §§ 801–808.

58. Press Release, French Hill Chairman, *McHenry Highlights Similarities Between CFPB's 1033 Proposal & Republicans' Data Privacy Act of 2023*, House Comm. on Fin. Serv.'s (Dec. 18, 2023), https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409081.

rationale for the proposed changes, followed by an opportunity for public comments to be submitted and a final rule with accompanying supplementary information addressing the feedback received and explaining the agency's approach to its changes. Indeed, new leadership at the CFPB could present the best opportunity for the rule to be further refined to address the many open issues discussed above. The CFPB could also issue guidance and other materials, such as a small entity compliance guide, to help the industry comply with the rule.

D. Additional CFPB Rulemaking Activity.

— More products: The CFPB intends to expand the scope of its rules—through additional, incremental rulemakings—to cover other consumer financial products or services, potentially including mortgages, auto loans, and student loans. Incremental rules of this sort are also an opportunity for the CFPB to refine other aspects of the final rule.

— Data broker rules: The CFPB proposed a rule to regulate the activities of data brokers under the FCRA.[59] If that rule is finalized as proposed, it could impact data aggregators to the extent they are viewed as "consumer reporting agencies"[60] and authorized third parties to the extent they are viewed as "users" of a consumer report when accessing 1033 covered data. While the CFPB acknowledged several potential areas of overlap, the application of the FCRA's framework

59. *See* Protecting Americans from Harmful Data Broker Practices, *supra* note 55.

60. The proposed rule discusses a variety of activities that could be viewed as assembling or evaluating data, causing the entity performing the activities to be considered a "consumer reporting agency" subject to FCRA. In discussing these activities, the proposed rule states

> [A] person assembles or evaluates when the person collects information from a data source and then groups or categorizes it, regardless of whether the person alters or changes the information. . . . a person assembles or evaluates when the person collects information from a consumer's bank account and assesses it, such as by grouping or categorizing it based on transaction type. The CFPB understands that data aggregators often engage in such activities. The CFPB understands, for instance, that, when a data aggregator collects information from a consumer's bank account, the data aggregator may apply its own taxonomy to group or categorize the collected information. To take just one factual scenario, a data aggregator that collects bank account information pursuant to consumer authorization in connection with a loan application may group or categorize deposits or withdrawals by type of income or expense, such as 'rent' and 'loan repayment,' prior to sharing it with the lender. In doing so, the data aggregator assembles or evaluates the information. Protecting Americans from Harmful Data Broker Practices (Regulation V), 89 Fed. Reg. at 101426.

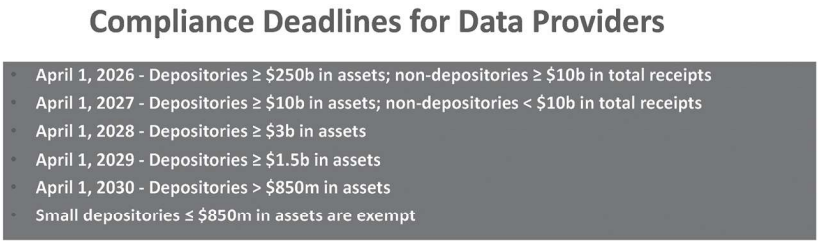
to consumer-permissioned data sharing under 1033 is yet another area of ambiguity that the CFPB has not resolved.

Despite the uncertainty presented by these headwinds, and even if the final rules were set aside by the CFPB or a court, the demand for consumer-authorized access to data is expected to continue growing. Data providers, data aggregators, and authorized third parties will need to address many of the policy issues covered in the final rule to ensure consumers are well informed, apply appropriate third-party risk management controls, including data security requirements, and enter bilateral data sharing arrangements to appropriately apportion liability for the variety of risks presented.

VIII. The Path Forward: Meeting Compliance Deadlines and Engaging with Standard Setters

A. Compliance Deadlines.

Data providers subject to the final rule must prepare to comply with a series of complex obligations within the following compliance deadlines:



Unlike data providers, compliance deadlines for third parties are not explicitly set forth in the final rule, leaving open the question of when they must comply. Third parties might conclude that the rules become applicable on the effective date of the rule, which is January 17, 2025, or on the first effective date for data providers, which is April 1, 2026.[61] Third parties could also wait to comply with the rule until data providers require them to comply with the rule as a condition to accessing data, which would likely

61. *See* Required Rulemaking on Personal Financial Data Rights, *supra* note 3 at 90838.

result in bifurcated data access patterns between data subject to 1033 and not subject to 1033.

A series of key questions that should be asked by entities contemplating compliance with the rule are included in the Appendix.

B. Engaging with Standard Setters.

The final rules prescribe requirements for recognized standard setters to be open, transparent, and balanced, among other things. Given the potential for the standards they issue to carry significant weight in determining whether a company is complying with the CFPB's rules, influencing those standards will be of utmost importance to data providers and third parties, as well as other interest groups representing impacted stakeholders, such as consumer advocacy groups.

Now that the CFPB has recognized the Financial Data Exchange ("FDX") as the first standard setter under its 1033 rules,[62] the race is on for their first "consensus standards" to be issued. The governance requirements established by rule seek to ensure that data providers and third parties have equal power in determining the content of these standards, and that non-commercial groups are consulted as well, with board resolutions requiring a two-thirds agreement.[63] FDX members can also submit change requests at any time and those requests must be considered using a similar process. Additionally, FDX is considering a service whereby it would evaluate whether an entity is in fact adhering to its standards and issue a certification, for use by the recipient, as evidence of compliance.

The first order of business for FDX will likely be to issue a consensus standard for data formats because, as discussed above, these standards are a fundamental component of an interoperable data sharing system.

Conclusion

Open banking's impact on consumer finance in the United States is evolving rapidly, offering both significant opportunities and complex challenges to be managed in the years ahead. The CFPB's final rules on Personal Financial Data Rights mark a pivotal step toward legitimizing consumer-authorized data sharing, promoting innovation, and enhancing consumer control over financial information. By transitioning from screen scraping to API-based data sharing, the industry is poised to improve security, interoperability, and operational efficiency.

62. *See* Interagency Guidance on Third-Party Relationships: Risk Management, *supra* note 28. The CFPB's recognition lasts five years, from January 8, 2025 until January 8, 2030. It states that the board must have balanced representation from data providers (up to twelve board seats), third parties (up to twelve board seats), and non-commercial groups (up to two board seats).
63. *Id*. (stating that all previously issued standards must be re-adopted by the FDX board).

However, the path forward is not without obstacles. Stakeholders must address many legal ambiguities, interoperability challenges, and operational complexities as new networks connecting data providers and third parties continue to evolve. Balancing innovation with consumer protection requires careful collaboration among all stakeholders, including recognized standard setters.

Despite these challenges, the persistently growing demand for open banking underscores its potential to support innovation, enhance financial inclusion, improve competition, and empower consumers. By addressing the issues outlined in this paper, the industry can unlock open banking's transformative potential while maintaining trust and achieving regulatory compliance, ensuring a sustainable future for open banking in consumer finance.