LEGAL UPDATES

PUBLISHED: OCTOBER 23, 2024

Open Banking Is Here: An Overview of Section 1033 of the Dodd-Frank Act

Services

Consumer Financial Services

Credit Unions

Industry

Financial Services & Capital Markets

Professional

CHRISTOPHER K. FRIEDMAN
NASHVILLE: 615.949.2252
CHRIS.FRIEDMAN@HUSCHBLACKWELL.COM

In a move that has been a long time in the making, the Consumer Financial Protection Bureau (CFPB) has finalized its comprehensive open banking rule. The rule implements Section 1033 of the Dodd-Frank Act and grants consumers the right to access their financial data and authorize third parties to access that data on their behalf. According to the CFPB, this data-sharing rule will empower consumers to shop for and switch financial service providers more easily, thereby fostering competition and innovation. Indeed, a system of open banking that allows consumer financial services data to flow more easily and efficiently could prove to be a catalyst for an already growing fintech industry. However, serious challenges await industry participants working to comply with the new regulatory regime, and many participants are already objecting to the scope of the new rule.

What is Dodd-Frank Act Section 1033?

Dodd-Frank Act Section 1033(a) and (b) provide that, subject to rules prescribed by the CFPB, 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, subject to certain exceptions. The information must be made available in an electronic form usable by consumers. In addition, Congress mandated in Section 1033(d) that the CFPB prescribe standards to promote the development and use of standardized formats for data made available under Section 1033. In June 2024, the CFPB finalized a separate rule addressing the data standard-setting component of Section 1033.

Who is covered in the 1033 Rule?

The rule applies to "data providers," which include depository institutions such as banks and credit unions, as well as non-depository institutions that issue credit cards, hold transaction accounts, issue devices to access an account, or provide payment facilitation services and specific "authorized third parties." However, in a change from the proposal, small depository institutions (i.e., those with $850 million or fewer in assets) are exempt from the rule.

One surprise: In a change from the proposal, the CFPB **included** digital wallet providers and payment apps as data providers. Moreover, the rule notes that digital wallet providers constitute "data providers" even when they are only facilitating pass-through payments. This means that many of the most popular fintech payment platforms and wallet providers will be subject to the open banking regime.

What is covered in the 1033 Rule?

"Covered data" encompasses information about transactions, costs, charges, and usage related to consumer financial products and services. These include information about account balances, historical transaction information (24 months) in the control or possession of the data provider, terms and conditions, upcoming bills, and Regulation E payment initiations. Consumers can authorize third parties to access this data, provided they adhere to strict security and data use limitations.

What does this mean for "data providers"?

The final rule mandates that data providers make covered data accessible to consumers and authorized third parties upon request, ensuring the process is reliable, secure, and competitive. Data must be provided in a standardized, machine-readable format, and data providers are required to meet a minimum response rate for data requests. Restrictions on request frequency are prohibited, and data providers generally are prohibited from utilizing "screen scraping" as a method for granting data access to third parties under the rule. Furthermore, the rule prohibits any fees or charges related to consumer and third-party data access. Data providers are required to have written policies and procedures and retain records that are evidence of a data provider's actions in response to a consumer's or third party's request for information for at least three years after a data provider has responded to the request.

What does this mean for "third parties"?

For third parties to become "authorized," they must seek data access on behalf of consumers to provide requested products or services, furnish an authorization disclosure with key terms, and ***obtain the consumer's express consent***. Third parties must limit the collection, use, and retention of data to what is necessary for the requested services, excluding targeted advertising and

cross-selling. The rule sets a maximum data collection duration of one year, requiring renewed consumer authorization after that point. Moreover, third parties must certify to have written policies for data accuracy, apply an information security program in line with the Gramm-Leach-Bliley Act (GLBA) Safeguards Framework, and provide consumers with copies of authorization disclosures and a method to revoke consent. Data aggregators can assist third parties with authorization procedures but must certify compliance with third-party obligations. Third parties are required to retain records for a minimum of three years.

Compliance dates

Compliance with the rule will be phased in over several years. Larger providers are required to comply by April 1, 2026, while smaller providers have until April 1, 2030. The CFPB has also established qualifications for recognized industry standard-setting bodies, which can issue standards to aid compliance with the rule.

Industry concerns and support

There have already been strong reactions—both positive and negative—by industry stakeholders. Many of the fintech trade associations are generally supportive of the new rule, while recognizing some potential problems regarding some of the rule's details. For instance, Penny Lee of the Financial Technology Association says that the new rule is a "win for consumers, guaranteeing their right to own and securely share their financial data. This rule will increase competition, improve consumers' choices, and drive momentum for future innovations that benefit consumers—like cash flow underwriting, stronger fraud tools, pay-by-bank, and personalized financial services—while fostering greater trust in the financial ecosystem."

The American Fintech Counsel (AFC) took a more critical approach. Specifically, AFC Senior Vice President and Head of Policy and Regulatory Affairs, Ian P. Moloney, said that while the trade group "appreciates the monumental effort . . . to establish a robust Open Banking Framework," the trade group was "deeply concerned" about the Bureau's decision to finalize the rule without considering and revising provisions related to the secondary use of data for cross selling financial products and marketing. "[R]esponsible fintech companies and innovative banks can leverage consumers' data to offer improved products and services to historically underserved communities and provide additional responsible services beyond those the consumer initially sought." The AFC also criticized the rule's annual reauthorization requirement.

On the other hand, the banking trades were unanimously negative in their assessment of the rule. According to Housingwire, Community Bankers Association president and CEO Lindsey Johnson has taken the position that the CFPB "exceeds its statutory authority [by] enabling thousands of third parties to access consumer data." She also stated that "[t]his has created an even less durable final

rule that does not reflect market, technological, and practical realities." According to the American Banker, American Bankers Association president and CEO Rob Nichols commented that "what began two administrations ago as a collaborative exercise in securing consumers' personal financial data has evolved into a press-release-driven, political exercise based on the false premise that consumers lack choices and a misunderstanding of whether Dodd-Frank grants CFPB the authority to radically reshape the financial services marketplace."

In addition, many banks are concerned about the fact that the final rule did not address data providers' concerns about allocating liability for data privacy and security lapses. They claim the final rule did not address commenters legitimate concerns that banks could be left on the hook for actions that are the fault of nonbank parties.

And, unsurprisingly, there is **already** litigation over the new rule. On October 22—the day the CFPB released its Section 1033 rule—the Bank Policy Institute (BPI), the Kentucky Bankers Association, and Forcht Bank, N.A. filed a lawsuit against the CFPB challenging the final rule in District Court in Kentucky. According to the BPI, the CFPB exceeded their statutory authority and violated the Administrative Procedure Act in various ways. According to the complaint, the rule

Requires no oversight of third parties who are using customer banking data, thereby leaving it up to banks to ensure the protection of sensitive customer information,

Increases the likelihood of fraud and scams by "failing to address weak safeguarding practices,"

Does not outright eliminate "unsafe" practices such as screen scraping,

Does not hold third parties accountable for data security,

"[A]llows third parties to profit, at no cost, from systems built and maintained by banks," and

"[I]mposes an unreasonable implementation timeline.

The lawsuit, filed in the U.S. District Court for the Eastern District of Kentucky, requests injunctive relief.

Flash webinar on Dodd-Frank 1033

REGISTER NOW

Husch Blackwell's Christopher Friedman and Mike G. Silver will be presenting a webinar on the CFPB's open banking rule on **Friday, November 1, 2024, from Noon to 1:00pm CT**. They will cover key aspects of the rule, including who and what is covered, consumer benefits like seamless switching and potentially better rates, the challenges and opportunities the rule presents for different

market participants, major changes from the proposal, and compliance timelines. Don't miss this opportunity to understand how these changes will shape the future of open banking.

This webinar will be beneficial to professionals in the financial services sector who work with consumer financial data. This includes representatives from medium-to-large-sized banks and credit unions, non-bank lenders, small-to-medium-sized business finance companies, payment app providers, and other service providers in the financial services industry. Additionally, companies offering underwriting and loan analytics solutions will find this session particularly helpful.

This program is pending approval for Colorado, Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, Tennessee, Texas, and Wisconsin continuing legal education credit.

This webinar is complimentary; however, registration is required. Unable to join us at the scheduled date and time? Register anyway and we will email the recording to you.