Data Aggregation - 1033

Ryan T. Miller | rmiller@aba.com | 202-663-7675 January 2025

Issue Update

Section 1033 of the Dodd-Frank Act gives consumers the right to access and share their financial records in a standardized electronic format, with some exceptions. Such access could be direct by the consumer or by authorized third parties, using entities known as data aggregators as intermediaries. Use cases for data sharing include budgeting tools, income verification, and digital wallets.

The CFPB finalized a rule implementing 1033 in October 2024. It was immediately challenged in a lawsuit filed by a Kentucky community bank, the Kentucky Bankers Association, and the Bank Policy Institute (the case is still pending). The rule applies to Regulation E accounts, Regulation Z credit cards, and digital wallets connecting them. It mandates data providers to build and maintain, at their own cost, an interface for direct consumer access as well as a developer interface for authorized third parties. In addition, data providers must create policies and procedures, disclose certain information, retain records, and more. The rule also contains requirements for authorized third parties and data aggregators, such as managing express informed consent (for a maximum duration of one year subject to renewal and revocation), creating policies and procedures, providing disclosures, and using/sharing/retaining information only as reasonably necessary to provide the consumer's requested product or service (with certain exceptions such as fraud prevention).

Finally, the rule establishes a recognition process for standard-setting organizations to offer evidence of compliance with certain substantive regulatory requirements. Since 2018, financial institutions, fintechs, and aggregators have collaborated through an entity called the Financial Data Exchange (FDX) to develop API and technical standards to support secure data sharing. FDX has applied for recognition by the CFPB.

The final rule has several issues that were left largely unremedied from the proposal: the prohibition on data providers to recoup costs; tensions between sharing and risk management; inclusion of problematic data fields such as payment initiation (which will accelerate "pay-by-bank"); a lack of a meaningful liability regime in the event of unauthorized activity or data breaches; failure to outright ban screen scraping (although the preamble does permit it to be blocked as long as there is a compliant developer interface); and a short compliance runway for the largest banks. On the positive side, the final rule clarifies that data providers are not furnishing under the Fair Credit Reporting Act when complying with 1033.

Why it Matters To Your Community

Banks support their customers' ability to access and share their financial data in a secure, transparent manner that gives the customer control. Screen scraping is a dangerous practice that leaves consumers' credentials and account information subject to security risks and fraud, and it is important the industry adopt more secure data sharing methods. However, the CFPB's 1033 rule is flawed and puts consumer data at greater risk while imposing significant costs on banks.

Recommended Action Items

- **Urge the CFPB to delay implementation and finalize a CFPB rule to supervise data aggregators before significantly overhauling the 1033 rule to address scope, liability, and cost.** These changes are critical to ensure consistent protections and outcomes for consumers.
- **Urge the CFPB to recognize the Financial Data Exchange (FDX) as a standard setting organization to evidence compliance with data format requirements.**