OpenFinity Nov 7, 2024 6 min read

CFPB 1033: 4 Areas Where Compliance and Legal Teams Should Pay Close Attention

Updated: Dec 2, 2024

On October 22, 2024, the Consumer Financial Protection Bureau (CFPB) published its final rule under Section 1033 of the Dodd-Frank Act, a complex nearly 600-page regulation highly anticipated by the U.S. financial industry.

However, the rule may benefit from further guidance or clarifications, specifically around liability boundaries, outlining safe harbor protections for data providers, and privacy and security requirements for third parties.

> **"The Future of Privacy Forum[1] believes the 1033 rule is an important step for open banking in the U.S. Stakeholders should pay careful attention to the new rules and obligations for privacy. By establishing data collection, use, and retention limitations on third parties, it creates obligations that are new in the financial sector, and on parties that may also be new to the financial regulatory landscape. How these obligations are interpreted, disclosed, overseen and enforced will be pivotal to whether consumers' privacy is truly protected as the rule envisions."**

For the compliance and legal teams of a financial institution impacted by Section 1033, here are four areas that deserve your close attention and why. While the following reflects our analysis, financial institutions should review these carefully and seek the opinion and counsel of attorneys and organizations specializing in privacy and regulations.

1. Liability and Risk Management

What are the specific obligations and liability boundaries for banks versus third-party data aggregators or fintechs, especially in cases of fraud, unauthorized transactions, or data breaches? Will there be clear warranties set by private network rules or activities-specific guidance from prudential bank regulators?

2. Data Use Permissions

What guidelines or limitations are there on uses of consumer-authorized data by third parties, specifically concerning product improvements, research, and anti-fraud measures?

Nota 1: The CFPB retained its general limitation prohibition against secondary data uses. However, there are some permissible secondary uses—to comply with the law (e.g., responding to subpoenas or regulators), to prevent fraud, to conduct requested transactions, and as reasonably necessary to improve the product or service the customer requested.

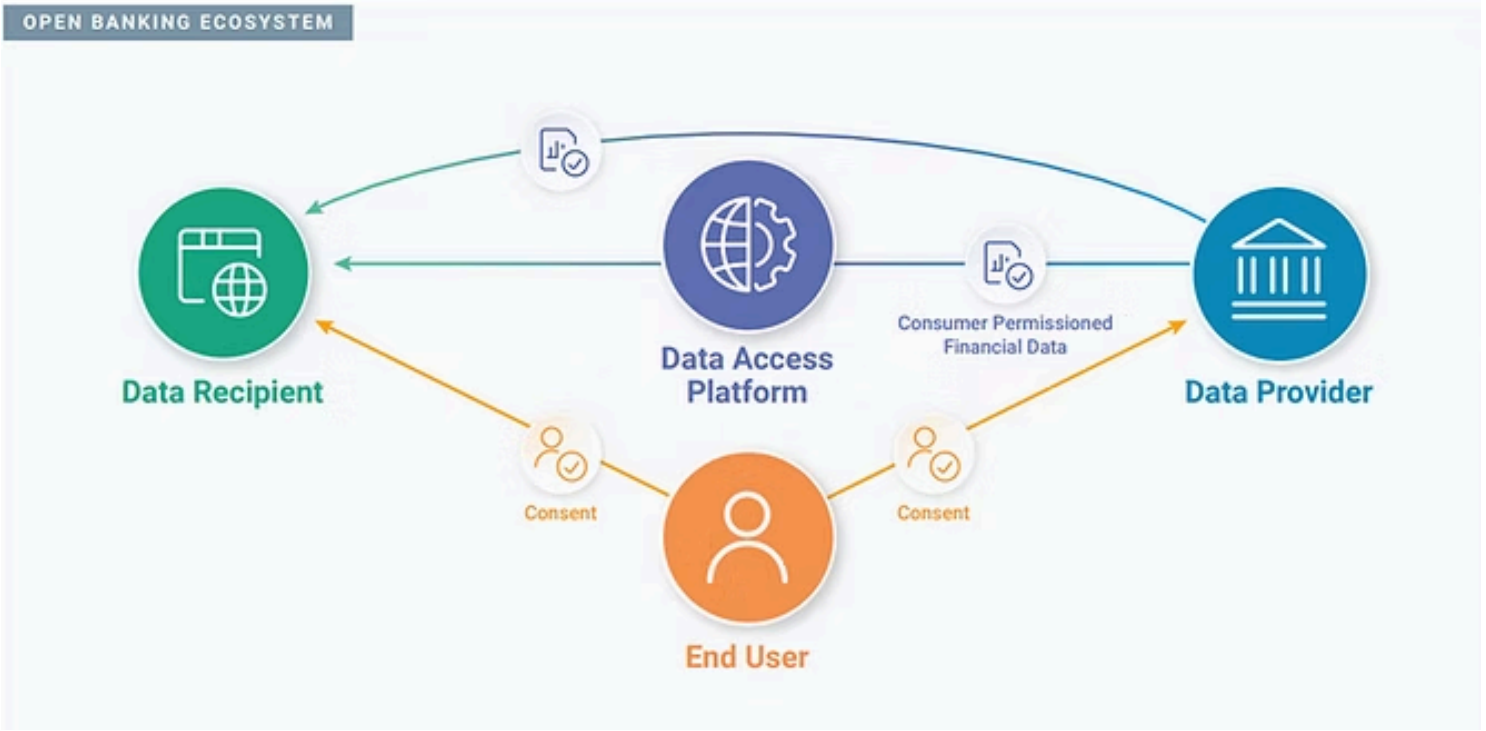
Nota 2: The CFPB allows other uses (including targeted advertising, cross-selling, and sale) to be done if clearly a primary part of the requested product or service. It depends on context. In this way, someone could authorize the use of their information for research purposes. The CFPB also says "standalone" products or services do not necessarily have just a single attribute—they can be combined—the key is whether the consumer can reasonably be expected to understand what they are agreeing to. They touch upon this at length in the preamble.

3. Data Revocation and Security Obligations

What is the protocol for handling revoked data access authorizations? What obligations do data providers and third-party fintechs have for ensuring data security, particularly if they are using intermediaries or aggregators?

4. Are there any conflict or overlaps with other Regulations?

For instance, 1033 may intersect with other regulations, such as REG E, FCRA, and Reg P, particularly around issues of consumer rights, liability, and error resolution in electronic transactions.



Source: Financial Data Exchange: **'Getting Started with Open Banking'**

Digging CFPB 1033 Further

Because the new CFPB Section 1033 introduces complex data-sharing requirements, liability can become ambiguous when multiple parties, including banks and third-party aggregators, handle sensitive consumer data.

Here's why this is potentially unclear:

1. Multiple Parties in Data Access:

With Section 1033, consumers can authorize third-party providers to access their financial data. This data may pass through aggregators, banks, and fintechs, creating a multi-layered chain where data could be mishandled, misused, or accessed by unauthorized parties. If a data breach or unauthorized transaction occurs, it may be unclear who bears responsibility.

2. Consumer Authorization and Third-Party Access:

Section 1033 allows consumers to authorize third-party providers, which the CFPB distinguishes as acting on behalf of the consumer, not as service providers to the bank. This distinction could mean that banks may not have the authority to control or assess all risks posed by third-party fintechs, complicating liability if those third parties mishandle data.

3. Lack of Specific Safe Harbor Protections:

Many regulations include safe harbor provisions, which provide protection from liability for institutions that meet specified compliance standards. However, the CFPB's rule doesn't clearly outline safe harbor protections for banks or aggregators that comply fully with data security and consent requirements. Without such protections, banks could bear responsibility even if they follow all compliance protocols, particularly if unauthorized access or fraud occurs due to third-party vulnerabilities.

4. Unresolved Questions on Fraud Liability:

The rule could benefit from more specific guidance on fraud and liability responsibilities. For example, if a third-party provider is involved in a data breach or unauthorized transaction, it's not fully clarified if liability rests solely with the third party or if the originating bank shares responsibility. Similarly, it's unclear who would handle consumer dispute resolution in cases of third-party access issues.

What about Reg E potential Overlaps?

Regulation E (Reg E), which implements the Electronic Fund Transfer Act (EFTA), may intersect with Section 1033, particularly around issues of consumer rights, liability, and error resolution in electronic transactions.

Key areas of potential overlap or interference between Reg E and Section 1033 include:

1. Consumer Liability for Unauthorized Transactions:

Reg E limits consumer liability for unauthorized electronic fund transfers, while Section 1033 introduces new data-sharing obligations for banks and third-party providers. There may be a need for further clarification on who bears liability under Section 1033 if an unauthorized transaction occurs due to data shared with a third-party fintech app.

2. Error Resolution and Dispute Handling:

Reg E requires financial institutions to investigate and resolve errors within a specific timeframe. With Section 1033 allowing broader data-sharing with third parties, it is important to clarify whether and how banks or third parties will be responsible for errors in transactions initiated through shared data.

3. Consumer Disclosure and Consent Requirements:

Reg E mandates that consumers be informed about their rights and liabilities regarding electronic transactions. Section 1033 also emphasizes informed consent for data-sharing. Aligning the disclosure requirements under Reg E with the consent and authorization requirements under Section 1033 may help avoid redundant or conflicting consumer notifications.

It is important to note that the CFPB declined to amend Regulation E at this time. We believe that it is endorsing a view that private networks should create a framework to apportion liability for unauthorized activity. They do not believe this question should be settled in bilateral Data Access Agreements between data providers and third parties.

What About Other Regs?

Other regulations, such as Regulation Z (Reg Z) and several others, may intersect with Section 1033. Here are some examples and the areas where potential overlaps or interference could arise:

1. Regulation Z (Truth in Lending Act - TILA)

Consumer Liability**: Reg Z limits consumer liability for unauthorized credit card transactions. Section 1033's provisions for data-sharing could introduce new liability considerations if third-party data access leads to unauthorized or fraudulent credit transactions.

2. Regulation P (Privacy of Consumer Financial Information)

Reg P mandates that financial institutions protect consumers' personal financial information and disclose how it is shared. Section 1033 also requires that consumers provide authorization before sharing data with third parties, so aligning privacy and consent standards could help avoid conflicting requirements.

3. Regulation V (Fair Credit Reporting Act - FCRA)

Reg V governs the accuracy of consumer information shared by credit reporting agencies. If Section 1033 data includes consumer credit information shared with third parties, consistency between data accuracy and dispute processes under Reg V and Section 1033 could be crucial.

Thanks to comments and recommendations share by organizations like the American Bankers Association with the CFPB during the review period, data providers are not furnishers under the Fair Credit Reporting Act/Reg V when making information available under 1033 (even if the data aggregator is a consumer reporting agency).

4. Regulation DD (Truth in Savings Act - TISA)

Reg DD mandates transparent disclosures about account terms, fees, and interest rates for deposit accounts. If Section 1033 involves data-sharing related to deposit accounts, consistency between

Reg DD disclosures and information provided to third-party data aggregators might be necessary to avoid consumer confusion.

Conclusion

CFPB 1033 isn't perfect, and most likely further guidance and even amendments will be needed. Compliance officers and legal counsels impacted by 1033 should seek guidance from privacy and legal experts to clarify these areas.

Despite these challenges, 1033 is a significant step forward to bring the U.S. on par with global counterparts.

Additional information:

- if you are an American Bankers Association, you can also access the Staff Analysis by Ryan T. Miller published on Nov 4, 2024: Final Rule Regarding Personal Financial Data Rights (Dodd-Frank Act Section 1033)
- CFPB Section 1033 : Final Rule -Key Takeaways and New Compliance Deadline

[1] The Future of Privacy Forum (FPF) is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies. FPF is focused on advancing responsible data practices and has deep expertise regarding privacy and data protection, including concerning the privacy implications of open banking.