Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# CFPB Financial Data Principles: Whose Data Is It Anyway?

By **David Beam, Jonathan Jaffe, Jeff Taft and Kendall Burman**
November 13, 2017, 11:53 AM EST


David Beam


Jonathan Jaffe


Jeff Taft


Kendall Burman

On Oct. 18, 2017, the Consumer Financial Protection Bureau released guidance that is intended to provide the bureau's "vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value."[1]

Many companies in the "fintech" space have developed products that provide a user interface that allows customers to access information about accounts at other financial institutions that have no relationship with the fintech provider — and even to initiate transactions with the account at the unrelated financial institution. These products often allow consumers to aggregate information from multiple accounts at different financial institutions in a single user interface. They also give consumers more flexibility to choose the user interface that they prefer. These products also frequently enable or facilitate "contextual commerce" transactions (jargon for consumer purchases of goods and services from a variety of merchants in an environment that the consumer uses primarily for a purpose other than shopping, e.g., on a social media platform).

Additionally, although aggregation of financial account information from multiple entities is a concept that has been around for some time, it has recently resurfaced as an issue because of the entry into the marketplace of a new generation of fintech providers, which differ from the established, and typically more stringently regulated, financial institutions.[2] The products and services offered by this new generation of market participants has raised new questions around consumer financial data, including questions related to privacy, security and accuracy, as well as concerns around improper payment authorization and consumer dispute mechanisms.

Many people in the financial industry (including account-holding financial institutions) endorse the idea of giving consumers more flexibility to decide how they will interface with their financial accounts. But most people in the financial industry (including fintech companies that provide the products and services that give consumers this flexibility) also agree that there are a number of important issues related to cybersecurity, privacy and fraud prevention that need to be considered. For example, how should a financial institution verify that its account holder knowingly authorized the fintech provider to access the account or initiate the transaction? Is the provider's representation that it has received the account holder's authorization enough — or should the financial institution

employ a "trust but verify" process (which might include directly obtaining an account holder's consent for the financial institution to give the provider account access)? May financial institutions adopt more rigorous authorization and security protocols than the minimum required by law — and, if so, at what point do measures adopted to protect the financial institution's customers from unscrupulous providers become so restrictive that they impermissibly undermine a consumer's ability to access his or her accounts in whatever reasonable manner the consumer chooses?

The remainder of this article is divided into three parts:

- Background: covering the issues that the guidance addresses and tracing the history of the guidance.

- Outline of the principles: a detailed description of the guidance.

- Observations and potential implications: observations on the guidance and what it may mean for consumers, fintech companies and the financial services industry.

**Background**

Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act states that, "[s]ubject 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."[3]

The meaning of this provision has been the subject of debate since Dodd-Frank was enacted. Generally speaking, the following two questions have been the crux of contention:

- Does this provision require a covered person to facilitate a consumer's access to account information through any reasonable means chosen by the consumer — or does it only require a financial institution to make such information available to the consumer through reasonable means of the financial institution's choosing? The provision clearly prohibits a financial institution from withholding account information from a consumer (subject to a variety of exceptions in Section 1033). But many financial institutions have argued that it does not require financial institutions to actively facilitate, or even allow, access through every method a consumer might desire.

- Does Section 1033 give the bureau the authority to issue rules that require a financial institution to provide account access through certain means or under certain circumstances? Section 1033 does appear to authorize the bureau, at least by implication, to issue regulations related to account access. Some people have argued that the rulemaking clause only permits the bureau to issue rules that limit a financial institution's obligations under Section 1033 — not to require the financial institution to do anything. The basis for this argument is that the covered person's obligations under Section 1033 are "subject to" rules that the bureau prescribes (not, for example, "in accordance with" rules prescribed by the bureau).

Early CFPB comments on Section 1033 suggested that the bureau interpreted its provisions to impose

broad obligations on account-holding institutions. In October of 2016, Director Richard Cordray noted that the CFPB was "gravely concerned by reports that some financial institutions [were] looking for ways to limit, or even shut off, access to financial data. [The CFPB believes that] consumers should be able to access this information and give their permission for third-party companies to access this information as well."[4] Prior to Cordray's statement, some large banks had reportedly taken steps to limit fintech firms' ability to access the financial information of consenting consumers due to concerns over data security and malware.[5]

The release of the principles below followed the CFPB's Nov. 14, 2016, request for information (RFI).[6] At the time, the CFPB declined to comment on whether it would adopt a new rule on data sharing but noted that it was monitoring the market for consumer harm related to this issue. The nonbinding principles put forth by the CFPB are likely an attempt to reconcile concerns over financial innovation, data security and other priorities without issuing more detailed guidance or promulgating a new rule.

**Outline of the Principles**

Recognizing that the market for aggregation services continues to develop, the CFPB developed a set of consumer protection principles. These principles cover the following areas:

1. Access — Consumers should be able to obtain timely information upon request about their ownership or use of a financial product or service from their product or service provider. Financial account agreements and terms should also "support safe, consumer-authorized access, promote consumer interests, and [should not] deter consumers from accessing or granting access to their account information." Access should not require consumers to share their account credentials with third parties.

2. Data Scope and Usability — Entities should allow consumers to share or authorize the sharing of financial data that includes any transaction, series of transactions, or other aspect of consumer usage; the terms of any account, such as a fee schedule; consumer costs, such as fees or interest paid; and consumer benefits, such as interest earned or rewards. Information should be made available in forms that are readily usable by consumers and consumer-authorized third parties. Third parties with authorized access should only access the data necessary to provide the product(s) or service(s) selected by the consumer and only maintain such data as long as necessary.

3. Control and Informed Consent — Authorized terms of access, storage, use and disposal should be fully and effectively disclosed to the consumer, understood by the consumer, not overly broad, and consistent with the consumer's reasonable expectations in light of the product(s) or service(s) selected by the consumer. Terms of data access should include access frequency, data scope and retention period. Consumers should not be coerced into granting third-party access. Consumers should understand data sharing revocation terms and should be able to readily and simply revoke authorizations to access, use or store data. Revocations should be implemented by providers in a timely and effective manner and, at the discretion of the consumer, provide for third parties to delete personally identifiable information.

4. Authorizing Payments — Authorized data access, in and of itself, is not payment authorization. Product or service providers that access information and initiate payments should obtain separate and distinct consumer authorizations for these separate activities. Providers that access information and initiate payments may reasonably require consumers to supply both

forms of authorization to obtain services.

5. Security — Consumer data should be accessed, stored, used and distributed securely. Consumer data should be maintained in a manner and in formats that deter and protect against security breaches and prevent harm to consumers. Access credentials should be similarly secured. All parties that access, store, transmit or dispose of data should use strong protections and effective processes to mitigate the risks of, detect, promptly respond to and resolve and remedy data breaches, transmission errors, unauthorized access and fraud and should transmit data only to third parties that also have such protections and processes. Security practices should be adapted to encompass new threats as they emerge.

6. Access Transparency — Consumers should be informed of, or able to readily ascertain, which third parties they have authorized and which are accessing or using their financial information. The identity and security of each such party, the data they access, their use of such data and the frequency at which they access the data should be reasonably ascertainable to the consumer throughout the relevant access and storage period.

7. Accuracy — Accessed data should be accurate and current. Consumers should be able to dispute and resolve data inaccuracies.

8. Ability to Dispute and Resolve Unauthorized Access — Consumers should have reasonable and practical means to dispute and resolve instances of unauthorized access and data sharing, unauthorized payments conducted in connection with or as a result of either authorized or unauthorized data sharing access and failures to comply with other obligations, including the terms of consumer authorizations. Consumers should not be required to identify the party or parties who gained or enabled unauthorized access to receive appropriate remediation.

9. Efficient and Effective Accountability Mechanisms — Commercial participants are accountable for the risks, harms and costs they introduce to consumers. Commercial participants should prevent, detect and resolve unauthorized access and data sharing, unauthorized payments conducted in connection with or as a result of either authorized or unauthorized data sharing access, data inaccuracies, insecurity of data and failures to comply with other obligations, including the terms of consumer authorizations.

**Observations and Potential Implications**

Focused on "the importance of consumer interests to all stakeholders in the developing market for services based on the consumer-authorized use of financial data," the bureau's guidance contains principles that are exactly that — principles, not hard and fast rules. To the bureau's credit, this guidance provides some insights into how the CFPB will analyze issues related to third-party account access. But as is highlighted below, there is still enormous room for disagreement about what actions the principles will require in any particular instance.

**Principles for All**

Most of the bureau's prior statements on third-party access to consumer account information have focused on financial institutions that limit access. However, the guidance also provides a number of principles for providers of services. For example:

- Under the second principle, the guidance says that third parties should only access the data necessary to provide the product(s) or service(s) selected by the consumer and only maintain such data as long as necessary.

- Under the third principle, the bureau reminds third parties about the need to obtain clear and informed consent from consumers, to ensure that the authorization addresses a number of specific items (such as access frequency, data scope and retention period) to limit the data the third parties access to the extent of the consent, and to provide meaningful consent revocation mechanisms.

- Under the fifth principle, providers have obligations to protect consumer data (including both account data obtained from financial institutions and the account access credentials) against security breaches.

Some of the principles also impose indirect obligations on providers or at least imply that financial institutions have some authority to impose certain obligations or limitations. For example, the sixth principle says that consumers should be able to ascertain which parties are accessing or using their financial data. Although this principle doesn't identify which party (the financial institution or the provider) has the obligation to make this information readily ascertainable, it appears to suggest that the financial institution is required to provide the consumer with information about who is accessing the account. And this, in turn, might imply that a financial institution can impose some kind of requirements on third parties to identify themselves.

**Conflicting Principles?**

One major weakness in the principles is that they do not acknowledge some of the significant tensions that can arise between individual principles or provide parties with much direction about how to weigh competing principles. For example, the principles make clear that financial institutions must tear down barriers that unreasonably block consumer access — yet remind them that they can't hold consumers liable for unauthorized transactions made possible by the elimination of these barriers.

Additionally, one of the data privacy concerns highlighted in the RFI was that data aggregators would obtain more information than they need in order to provide a stated product or service and, as a result, would expose this information to greater privacy and security risk.[7] This concern is reflected in the principle regarding data scope and usability. While the CFPB mentions the importance of innovation, this principle may limit new product development by discouraging fintech providers from obtaining consumer information as a means of determining how to develop, or whether to offer, additional services or innovations. In other words, the principles may make it more difficult for financial firms to broaden their product offerings based on aggregated financial information from consumers who already use their core product offerings.

**Integrated Approach**

No matter what one thinks about third-party access in general, a major weakness in the guidance is its failure to even acknowledge that financial institutions will — and must — factor in some principles unrelated to consumer protection when developing protocols for account access. For example, the bureau does not even mention a financial institution's obligations to combat money laundering and terrorist financing, and to ensure compliance with U.S. sanctions laws. Anti-money laundering (AML) and sanctions concerns could become especially important when a third-party is allowed to initiate

transactions on behalf of a consumer. As is always the case, sometimes the need to guard against fraud or financial crimes will take precedence over customer convenience. And there are some significant AML and sanctions compliance issues that financial institutions need to consider:

- How does a financial institution ensure that the third party has a user authentication mechanisms that is sufficiently robust to reasonably assure that the party accessing the account is the customer or authorized user whose identity the financial institution verified and periodically sanction-screens?

- Will third parties be required to provide the financial institution with information that the financial institution determines that it needs in order to effectively monitor for suspicious transactions?

- Can a financial institution require the third party to implement steps to ensure sanctions compliance or require the party to provide sufficient information for the financial institution to ensure this? For example, a financial institution generally will not allow a person to log in to the account (much less initiate transactions) with a computer that has a North Korean IP address — and it is likely that most financial institutions do not permit access through a TOR (The Onion Browser) exit node.[8] Can a financial institution require a third party to impose similar restrictions as a condition to accessing the account?

Even though the CFPB sometimes seems to regard potential harm to a financial institution (such as fraud losses) as a secondary concern, principles of safety and soundness and the prudential regulators require financial institutions to protect themselves from unacceptable risk exposure.

Additionally, some of the CFPB's principles may not align with guidance from other regulators and commonly accepted market practices and legal rights. For example, the CFPB's principles state that consumers should not be required to share account credentials with third parties to facilitate information sharing, but the Office of the Comptroller of the Currency expressly stated in its account aggregation guidance that banks may, and typically do, require customers to share account credentials.

The bureau's mandate is to protect consumers, so it is completely understandable that its guidance focuses on consumer protection principles. It would even be understandable if the CFPB didn't want to offer any thoughts on matters outside its expertise, such as AML and sanctions compliance or prudential standards. However, it is disappointing that the CFPB did not even acknowledge the broader regulatory ecosystem in which financial institutions operate, and that the bureau's statement of principles doesn't represent the universe of factors to consider.

**Binding Effect of the Principles**

The principles are not formal regulations, and the CFPB says further that the principles are not binding precedent, guidance or "intended as a statement of the Bureau's future enforcement or supervisory priorities." But it seems obvious that the principles could significantly influence how bureau examiners and enforcement attorneys will view data-sharing and aggregation services in the future.[9] This is not the first time the CFPB has released nonbinding "consumer protection principles" — it did so in July of 2015 when it released nine principles regarding payment systems.[10] Those principles focused on many of the same themes as the sharing principles, and those "nonbinding" principles still wound up being a harbinger of bureau enforcement actions against payments companies.

The financial data sharing and aggregation principles may similarly result in CFPB enforcement actions in this area. For example, in July 2015 the CFPB strongly emphasized data security concerns in the principles related to payment systems, even though data security has traditionally been considered a part of prudential regulation for many banks, securities intermediaries and insurance entities and within the Federal Trade Commission's jurisdiction for nonbanks. Shortly after the release of those consumer protection principles in July 2015, the CFPB brought an enforcement action against an online payment system alleging that the system deceived consumers about their data security practices and the safety of their online payment platform.[11] This represented the CFPB's first data security enforcement action, and illustrated how the bureau would leverage its broad authority over unfair, deceptive, and abusive acts and practices (UDAAP) to bring a data security claim by focusing specifically on deceptive representations about security practices.[12] In light of the similarities between these two sets of consumer protection principles, it is possible that the CFPB may seek to bring similar enforcement actions in the financial data sharing and aggregation context.

Further, the bureau's principles seem to imply that consumers have a right to instruct third parties that have received their data to delete that data. The principles also suggest that product and service providers must allow a third party authorized by the consumer to access that consumer's financial information.[13] Both of those suggestions impose significant obligations on service providers that may be in conflict with commonly accepted market practices and legal rights concerning consumer information and, in the case of mandatory sharing with consumer-authorized third parties, may add security concerns relevant to the required sharing of data with third parties.

Certain language in the data sharing principles may require further clarification. For instance, a consumer should generally be "able to authorize trusted third parties to obtain … information from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner."[14] This sentence implies that consumers can only authorize access if data sharing is for their "benefit" but does not clarify what that term means, how it would be assessed and who judges whether consumers benefit from any data sharing arrangement. It also remains unclear whether account providers must trust a third party in order to allow data sharing or whether "trust" is solely determined by the consumer.

**Conclusion**

The CFPB's principles related to consumer-authorized financial data sharing and aggregation signal uncertainty in the market and the continued potential for conflict between new and established financial services providers. In light of these principles (and assuming no dramatic shifts in the CFPB's priorities), it is possible that the CFPB may seek to impose additional regulatory obligations on market participants through a rulemaking under Section 1033 or its larger-participant authority and/or further expand the scope of its enforcement authority. A rulemaking would signify an attempt to police the interaction between fintech firms and banks in regard to data sharing and information security, which would represent uncharted territory for the CFPB.

---

*David L. Beam is a partner at Mayer Brown LLP in Washington, D.C. Jonathan D. Jaffe is a partner in Palo Alto, California. Jeff P. Taft is a partner and Kendall C. Burman is counsel in Washington, D.C.*

*Mayer Brown Washington, D.C.-based partners Laurence E. Platt, Rajesh De and Stephen Lilley, and associates Matthew Bisanz and James K. Williams also contributed to this article.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] CFPB, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017), http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf [hereinafter Principles]; see also CFPB, Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights that Inform the Consumer Protection Principles (Oct. 18, 2017), http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

[2] See, e.g., Office of the Comptroller of the Currency, Bank-Provided Account Aggregation Services, Bull. 2001-12 (Feb. 28, 2001).

[3] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111–203, §1033, 124 Stat. 1376, 2008 (codified at 12 U.S.C. § 5533).

[4] CFPB, Prepared Remarks of CFPB Director Richard Cordray at Money 20/20 (Oct. 23, 2016), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-money-2020/.

[5] Lalita Clozel, Cordray Reignites Bank-Fintech Fight After Comments on Data Sharing, Am. Banker (Oct. 25, 2016), https://www.americanbanker.com/news/cordray-reignites-bank-fintech-fight-after-comments-on-data-sharing.

[6] CFPB, Request for Information Regarding Consumer Access to Financial Records (Nov. 14, 2016),

http://files.consumerfinance.gov/f/documents/112016_cfpb_Request_for_Information_Regarding_Consumer_Access_to_Financial_Records.pdf [hereinafter Request for Information].

[7] See CFPB, Request for Information at 13.

[8] TOR stands for “The Onion Browser.” It is a system that allows people to use the internet anonymously. Needless to say, since the use of TOR prevents a financial institution from knowing the country from which the person is logging in — or anything else about the person at the other end — most financial institutions do not allow login access through TOR.

[9] CFPB, Principles.

[10] CFPB, Consumer Protection Principles: CFPB’s Vision of Consumer Protection in New Faster Payment Systems (July 9, 2015), http://files.consumerfinance.gov/f/201507_cfpb_consumer-protection-principles.pdf.

[11] Consent Order, In the Matter of: Dwolla, Inc., 2016-CFPB-0007 (March 2, 2016) http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf. Please see our earlier Legal Update discussing that action in detail.

[12] Id.

[13] CFPB, Principles.

[14] Id.