CFPB Issues Principles for Financial Data Sharing and Aggregation

**Overview:** On October 18, the Consumer Financial Protection Bureau (the “CFPB” or “Bureau”) released a set of non-binding principles (the “Principles”) designed to protect the provision, use, and aggregation of consumer-authorized financial account data. The guidance is aimed at both financial institutions that maintain primary source consumer account information in the first instance, as well as the myriad FinTech companies and other service providers that aggregate and rely upon consumer-granted access to such account data for the purpose of providing ancillary services to the consumer. (Such services could include, for example, an online bill pay service, or a service that aggregates data from multiple consumer financial accounts and presents that information in an easily digestible, summary fashion).

The Principles can be summarized as follows:

- **Access.** Consumers should be able to timely obtain—and authorize third parties to obtain—information about their ownership and use of financial products or services from their service providers. Consumers should have easy access to information about which third parties are accessing or using the data, even if authorized by the consumer.

- **Data Scope and Usability.** Financial account data subject to consumer-authorized access (e.g., account terms, fees or interest paid, realized consumer benefits, etc.) should be available in a usable format, and should be discarded by third parties once no longer needed. Consumers should be able to expect the data are accurate and current.

- **Control and Informed Consent.** Consumer disclosures authorizing access and use of financial information should be clear, understandable, and not overly broad. Consumers should never be coerced into granting third-party access, and should be able to easily revoke authorizations.

- **Security.** Consumer data must be accessed, stored, used, and distributed securely, and procedures must be in place to quickly detect and respond to potential data breaches. Companies should only transmit data to third parties that similarly have adequate security measures in place.

- **Disputes.** Consumers should have reasonable means to dispute and resolve both data inaccuracies and unauthorized access or sharing of their data.

These principles come on the heels of a 2016 CFPB request for information (RFI) from stakeholders regarding the consumer benefits and risks associated with financial services that rely on access to accounts and account-related information. The Principles were thus informed by a variety of stakeholders that responded to the RFI, including primary account “holders” like...
banks and credit unions; “aggregators” of such data; “users” of aggregated data to offer products and services to consumers; and consumer-protection advocates. As evidenced in these stakeholder responses, while account data users and aggregators tend to advocate for diverse and wide access to consumer-authorized financial data (so they can use the data to maximize the effectiveness of product and service offerings to consumers), account data holders and consumer advocates are often concerned about privacy and unauthorized use when companies access more data than is necessary for improving or offering financial products and services.

Outlook: Although the Principles, in large part, reflect common sense consumer protection standards that financial companies may already follow, in certain respects, the Principles may complicate the relationship between financial institutions and technology service providers, and may add undue burdens that frustrate the pace of technological innovation.

For example, with respect to data scope and usability, the Principles state that “third parties with authorized access 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.” It may not be automatically clear what is the minimum amount of data necessary to provide a particular product or service, and how long is appropriate for the service provider to maintain it. Service providers taking a cautious view may thus be dissuaded from collecting additional information that could potentially be used to expand and improve their product offerings. This, in turn, could have a detrimental impact on innovation.

As another example, with respect to data accuracy, the Principles assert that consumers should have “reasonable means to dispute and resolve data inaccuracies, regardless of how or where inaccuracies arise.” Read conservatively, this could mean that a FinTech company that is “downstream” from the original source of consumer financial account data must have mechanisms in place to field consumer disputes regarding the accuracy of information, even where the dispute arises at the primary source (financial institution) level. This would necessarily require enhanced coordination among financial institutions and such “downstream” FinTech companies, beyond what many in the field may already be doing.

Although the Bureau cautions that the Principles are neither binding nor intended to “alter, interpret, or otherwise provide guidance on” existing protections or to be interpreted as “a statement of the Bureau’s future enforcement or supervisory priorities,” there is ample reason to believe that CFPB examiners and enforcement attorneys may rely upon these Principles to determine whether particular conduct by financial institutions and their service providers rise to the level of unfair, deceptive, or abusive acts or practices (“UDAAP”) that are impermissible under the law. Consequently, the Principles deserve close attention by both financial institutions (whose consumer accounts may be subject to third party sharing), and the FinTechs and other companies that power the tools that rely upon this shared information.

Craig Saperstein, a member of NACHA’s Government Relations Advisory Group, is an attorney in the Public Policy practice of Pillsbury Winthrop Shaw Pittman LLP in Washington, D.C. In this capacity, he provides legal analysis for clients on legislative and regulatory developments and lobbies congressional and Executive Branch officials on behalf of companies in the payments industry. Deborah Thoren-Peden is a partner and member of the Financial Institutions Team at Pillsbury Winthrop Shaw Pittman LLP. She provides advice to financial institutions, bank and non-bank, and financial services companies. Andrew Caplan is an associate and member of the Financial Institutions Group and the Privacy, Data Security, and Information Use Focus Team at Pillsbury Winthrop Shaw Pittman LLP. He counsels and defends financial institutions, technology companies, and other clients that offer consumer products or services on a range of issues related to credit, payments, data privacy, cybersecurity, and e-commerce. The information contained in this update does not constitute legal advice and no attorney-client relationship is formed based upon the provision thereof.