Pepper Hamilton LLP
Attorneys at Law

CFPB's Financial Data Sharing Principles Impose New Burdens On Financial Institutions

CLIENT ALERT | November 16, 2017

Scott D. Samlin | samlins@pepperlaw.com
Avi D. Erdfarb | erdfarba@pepperlaw.com

ALL FINANCIAL SERVICES FIRMS THAT STORE CONSUMER DATA ARE AFFECTED BY THESE PRINCIPLES BECAUSE THEY COULD BE ASKED TO SHARE THAT DATA WITH CUSTOMERS OR THEIR AUTHORIZED THIRD PARTIES AT ANY TIME.

The Consumer Financial Protection Bureau (CFPB) recently published nine "principles" (available at http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf) and an accompanying "insights" (available at http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf) report regarding consumers who have authorized financial data sharing and aggregation (especially with fintech companies). The CFPB maintains that these principles are not "binding requirements or obligations," but also notes that they will "monitor closely developments in this market" and take "appropriate

actions to protect consumers." It seems plausible that these new principles will become de facto rules to which the CFPB will hold financial institutions accountable when conducting ongoing supervision, examinations and enforcement actions. However, with Richard Cordray's recent announcement that he will be stepping down as director of the CFPB, nothing about the agency is certain, and financial institutions should continue to monitor developments.

The principles focus on ensuring that consumers remain in control of their data and mirror many traditional information security principles — like those laid out in the Organisation for Economic Co-operation and Development's Privacy Framework and those codified in HIPAA. The principles describe a framework for customers' access to their financial information as well as who is using it, what information is being shared, how the information is safeguarded, and when the information is disposed of.

The nine principles are:

1. **Access:** Upon request, consumers, or designated third parties, should be able to obtain information about their ownership or use of a financial product from their providers in a timely and safe manner that does not require the consumers to share their account credentials with third parties. Financial account agreements and terms should support safe, consumer-authorized access and promote consumer interests, and should not seek to deter consumers from accessing or granting access to their account information.

2. **Data Scope and Usability:** This data may include transaction(s), usage, terms and conditions, and costs and benefits, and should be provided in a readily usable format. Authorized third parties should only have access to the data necessary to provide their products or services and should only keep the data as long as necessary.

3. **Control and Informed Consent:** Terms of access, storage, use and disposal of consumer data information should be disclosed to the consumer, understood by the consumer, and consistent with the consumer's expectations. Consumers should not be coerced into granting third-party access and should be able to easily revoke authorizations. Revocations should be executed in a timely manner, and the information should be deleted by the third party.

4. **Authorizing Payments:** Third parties must obtain a separate authorization to initiate a consumer payment, even if they have authorization to access the information.

5. **Security:** Consumer data (including access credentials) should be stored, accessed, used and distributed securely. Financial institutions and third parties with consumer data should have "strong protections and effective processes" that protect the data from breaches and other unauthorized access.

6. **Access Transparency:** Consumers should be able to easily determine which of their authorized third parties are actually accessing their information, along with their security measures, what data they access, how they use it, and how often they receive it.

7. **Accuracy:** The data should be accurate and current, and there should be a reasonable means to dispute and resolve data inaccuracies, regardless of how or where the inaccuracies arose.

8. **Ability to Dispute and Resolve Unauthorized Access:** Consumers should have reasonable ways to dispute and resolve unauthorized data access, even if they cannot identify who gained or enabled the unauthorized access.

9. **Efficient and Effective Accountability Mechanisms:** Financial institutions and third parties are accountable for the risks, harms and costs they introduce to consumers. Therefore, they should create incentives to prevent, detect and resolve unauthorized access to data.

Financial institutions and third-party service providers will need to closely coordinate, and may need to invest heavily, to fully implement these principles. Many of these requirements are vague and place the burden on the commercial entity to protect the consumer. This potentially heavy financial burden may have the unintended consequences of stifling innovation and conflicting with prudential regulatory requirements to operate safely and soundly. It also remains to be seen how these principles will apply to credit reporting agencies, which typically store consumers' information for decades.

This is not the first time the CFPB has issued nonbinding "principles." In 2015, it published nine nonbinding principles for faster payment systems (available at http://files.consumerfinance.gov/f/201507_cfpb_consumer-protection-principles.pdf) that also focused on data security. Less than a year later, the CFPB brought an enforcement action against Dwolla, Inc. (available at http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf) for Unfair, Deceptive, and Abusive Acts and Practices (UDAAP) violations related to misrepresentations of their data security program. The 2015 principles have become de facto rules that the CFPB enforces via its UDAAP authority, and it seems likely that the CFPB will endeavor to implement these "nonbinding principles" for data sharing in a similar manner. This second set of data security principles is also an affirmation that the CFPB is focused on financial institutions' information security, and it may seek to reissue the principles in a bulletin or a formal rulemaking. As such, it is important that financial institutions, third parties and fintech companies invest in, internalize and adapt themselves to these consumer protections.

Pepper Points

- The CFPB's nine principles for consumer-authorized financial data sharing and aggregation may become the unofficial basis of CFPB enforcement actions, most likely under its UDAAP authority.

- All financial services firms that store consumer data are affected by these principles because they could be asked to share that data with customers or their authorized third parties at any time.

- The CFPB is walking a fine line between protecting customers and stifling innovation.

- That said, the post-Cordray CFPB may take a completely different tack when deciding how best to regulate data sharing and aggregation.

- The principles require explicit consumer authorization for data sharing, which is absolutely revocable at any point.

- It is uncertain what, if any, impact this may have on data sharing that consumers cannot currently prohibit under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., and Regulation P, 12 C.F.R. 1016.

Pepper Hamilton has experience advising clients on all types of data privacy programs and regulatory regimes. If you have any questions, please contact the authors or another member of the Financial Services Practice Group.