ALERT MEMORANDUM

CFPB Takes Cautious Step on Principles for Consumer-Authorized Financial Data Sharing

November 3, 2017

On October 18, the Consumer Financial Protection Bureau (the "CFPB") released the Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (the "Principles"). The Principles represent a cautious step forward by the CFPB in providing guidance on how institutions holding customer accounts (such as banks) should share information with service providers, including "fintech" companies that obtain customer authorization to access their account information in order to provide services such as fraud screening, identity verification, personal financial management and bill payment. While U.S. regulators have expressed support for providing consumers with access to useful services and fostering competition in the financial services sector, additional sharing of data and the increase in data access points also creates additional risks from a cybersecurity and privacy perspective. In contrast to some jurisdictions, U.S. regulators continue to take a "wait-and-see" approach to new regulation in this space rather than pursuing a comprehensive, highly-prescriptive approach. While this gives industry time to continue working towards a self-regulatory solution that will be flexible and market-based, it leaves open for the moment questions about an uneven playing field for different market participants and whether consumer information is adequately protected by current market practices during this period of rapid change.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

WASHINGTON

Katherine Mooney Carroll
+1 202 974 1584
kcarroll@cgsh.com

NEW YORK

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

Diana Yu
+1 212 225 2444
diyu@cgsh.com

PARIS

Amélie Champsaur
+33 1 40 74 68 95
achampsaur@cgsh.com

LONDON

Gareth Kristensen
+44 20 7614 2381
gkristensen@cgsh.com

I. Introduction

The CFPB offers the Principles[1] as a set of ideals, setting forth a "common understanding of consumer interests" and expressing its "vision for realizing a robust, safe, and workable data aggregation market." The Principles reflect input received by the agency following its publication of a Request for Information in November 2016[2] (the "RFI"), in which the CFPB solicited feedback from industry stakeholders to better assess the data aggregation services landscape and the associated benefits and risks. The CFPB released a summary of stakeholder insights[3] on the same day as the release of the Principles. The Principles cover nine topics: data access, data scope and usability, consumer control and informed consent, authorized payments, data security, access transparency, accuracy of data, consumer ability to dispute and resolve unauthorized access and accountability mechanisms.

II. The CFPB Approach

1. Non-Binding Nature

Although the Principles are explicitly "not intended to alter, interpret or otherwise provide guidance on" the scope of existing statutes and regulations that may already apply to certain actors in this market and do not "establish binding requirements or obligations relevant to the Bureau's exercise of its rulemaking, supervisory or enforcement authority," they will certainly be viewed as relevant by companies seeking to identify best practices and develop industry-wide voluntary approaches to the topics addressed. The CFPB's press announcement[4] suggests that the Principles should be considered by "all stakeholders that provide, use, or aggregate consumer-authorized financial data." Financial companies in the U.S. are generally subject to regulations relating to data privacy and security promulgated under the Gramm-Leach-Bliley Act (the "GLBA")[5] and applicable state regulations,[6] but the scope of such regulations does not cover all fintech companies in the financial data aggregation service space. For fintech companies that are not subject to existing federal data privacy and security regulations, the Principles provide a very broadly drafted, non-binding outline of the CFPB's views of how certain business practices should be conducted to protect consumers.[7] For companies that are already currently subject to the GLBA or other federal or state regulations, the Principles add another layer of informal guidance to consider.

[1] To view the full text of the Principles, *see* http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[2] To view the full RFI, *see* http://files.consumerfinance.gov/f/documents/112016_cfpb_Request_for_Information_Regarding_Consumer_Access_to_Financial_Records.pdf.

[3] To view the full summary of stakeholder insights, *see* http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf (the "Stakeholder Insights").

[4] *See* https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/.

[5] The GLBA's data sharing and security standards apply to financial institutions, which are defined as "any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12." *See* 15 U.S.C. § 6809. The GLBA empowers several federal agencies (including the CFPB, FRB, OCC, FDIC, NCUA, CFTC, SEC and FTC) to implement regulations addressing data security and privacy and enforce them against entities subject to their respective jurisdictions. *See* 15 U.S.C. § 6804 and 15 U.S.C. § 6805. Whether a fintech company is subject to GLBA regulations will depend on the nature of its activities.

[6] For example, the state of New York's new cybersecurity regulations apply to all individuals and companies operating under a license, registration, charter, certificate, permit, accreditation or similar authorization under New York banking, insurance or financial services laws. *See* https://www.clearygottlieb.com/~/media/cgsh/files/2017/publications/alert-memos/nydfs-cybersecurity-regulations-take-effect-8-21-17.pdf. Forty eight U.S. states also have laws or regulations addressing breaches of personal data.

[7] Even where specific privacy regimes do not apply, the Federal Trade Commission Act enables the Federal Trade Commission to pursue actions against a broad range of companies if privacy or data security practices are deemed to constitute unfair or deceptive acts or practices. *See* 15 U.S.C. § 45.

2. Balancing Consumer Protection & Industry Innovation

The Principles attempt to strike a balance between protecting consumers with respect to data privacy and security, on the one hand, and supporting innovative and consumer-beneficial fintech products and services, on the other hand. The Principles indicate support for data sharing procedures that enable consumers to take advantage of such products and services and that foster competition, and demonstrate a bias against obstacles to data sharing that solely benefit account holding institutions (that may be reluctant to share data with third parties) but are not reasonably predicated on the consumer's own interests. For example, the "Access" principle suggests that an account holding institution should defer to a consumer's choice to authorize third parties to obtain account information for use on their behalf and that account holding institutions should support such access and not seek to deter consumers from granting such access. The "Data Scope and Usability" principle further suggests that financial data subject to consumer-authorized access should be made available in forms that are readily usable by consumer-authorized third parties. However, this is counterbalanced in the same principle by the statement that such third parties should limit their access to "the data necessary to provide the product(s) or service(s) selected by the consumer," and such data should only be maintained by such third parties for "as long as necessary." Therefore, it seems that some impediments to data sharing that are in the consumer's interest and not motivated by an account holding institution's anticompetitive objectives would be acceptable under the Principles.

Other principles are largely intended to protect consumers' data privacy and security, including, for example, the "Control and Informed Consent" principle, which advocates for proper disclosure of the terms of the authorized data access and the ability of consumers to revoke any authorizations previously granted by them. Notably, the CFPB acknowledges the potentially limited effectiveness of current disclosure practices, particularly as such disclosures multiply, but does not include any new guidance for how to address this challenge.[8] The "Security" principle suggests that "*all* parties that access, store, transmit or dispose of data 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 transmit data only to third parties that also have such protections and processes". In this regard, both the service provider (the "data aggregator") and the account holder are responsible for effectively guarding the privacy and security of the consumer information in their possession. Finally, the "Ability to Dispute and Resolve Unauthorized Access" principle states broadly that "*commercial participants* are accountable for the risks, harms, and costs they introduce to consumers," but it stops short of elaborating on the important issue of allocation of liability between an account holding institution and a service provider that is granted access, if the consumer were to suffer losses due to a breach at or through the service provider.

3. The Role of Regulators

In addition to striking the right balance between enabling consumer access to useful services and ensuring adequate data protection and consumer control over their information, regulatory authorities must also determine what role the government, as opposed to industry, should play in achieving that balance, particularly in light of the rapid pace of technological and behavioral change in this space. As the CFPB notes in the Stakeholder Insights, regulatory authorities have to consider whether to prescribe specific regulatory requirements or to allow industry to develop a consensus approach and effectively self-regulate, or to take an approach in the middle of the spectrum between those two. Here, the CFPB has taken a cautious approach (consistent with the broader regulatory approach to fintech thus far in the United

[8] The Stakeholder Insights acknowledge the concern expressed by many stakeholders that consumers may not read or understand the terms presented in disclosures when they authorize third-party access to their data.

States[9]), providing non-binding principles and suggesting that it is taking a "wait-and-see" stance for the moment, as industry tries to develop market-based solutions.

4. Comparison to Regulatory Approaches in the European Union & United Kingdom

The CFPB's non-binding, principles-based approach can be contrasted with the more prescriptive regulatory approach adopted by the European Union with its Second Payment Services Directive ("PSD2"). Beginning in January 2018, PSD2 will make it mandatory for banks to grant access (subject to customer consent) to their customers' online bank account to third party providers ("TPPs") such as fintech companies. The potential privacy and data security concerns associated with requiring banks to open up customer data are meant to be mitigated on a technical level by the strong customer authentication and secure communication protocols set out in the Regulatory Technical Standards that are being defined by the European Banking Authority. In addition, service providers, including data aggregators, are subject to strict, comprehensive European privacy laws (which contrast with the more sectoral approach in the U.S.), including the European Union's General Data Protection Regulation ("GDPR"), which comes into effect in May 2018.

The CFPB's approach can also be contrasted with that of the United Kingdom's Competition and Markets Authority ("CMA"), which issued reforms in 2016 designed to introduce greater competition in the UK retail banking market. One of the principal reforms mandated by the CMA was requiring the UK's nine largest banks to create and fund an Open Banking Implementation Entity that would develop "open data APIs," offering standardized information on UK banking products, and "read/write APIs," offering standardized APIs on which TPPs can build web and mobile applications to access customer data in accordance with PSD2.

III. Conclusion

The Principles represent a carefully calibrated step forward in U.S. regulatory efforts to address consumer privacy and data protection in the context of fintech and the rapidly evolving relationship between consumers, financial institutions and fintechs and other service providers. In contrast to some jurisdictions, U.S. regulators continue to take a cautious approach to new regulation in this space rather than pursuing a comprehensive, highly-prescriptive approach. While this gives industry time to continue working towards a self-regulatory solution that will be flexible and market-based, it leaves open for the moment questions about an uneven playing field for different market participants and whether consumer information is adequately protected by current market practices during this period of rapid change.

…

CLEARY GOTTLIEB

[9] *See, e.g.*, FINRA's report on Distributed Ledger Technology (http://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf); SEC OCIE's Risk Alert on Observations from Cybersecurity Examinations (https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf).