Consumer Financial Protection Bureau
1700 G Street, N.W., Washington, DC 20552

October 18, 2017

Consumer Protection Principles:
Consumer-Authorized Financial Data Sharing and Aggregation

In the Dodd-Frank Act, Congress instructed the Bureau to implement and enforce consumer financial law "for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive."[1] Congress further instructed the Bureau to exercise its authorities so that "markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation."[2]

For some time, a range of companies—many of them "fintech" companies—have been accessing consumer account data with consumers' authorization and providing services to consumers using data from the consumers' various financial accounts. Such "data aggregation"-based services include the provision of financial advice or financial management tools, the verification of accounts and transactions, the facilitation of underwriting or fraud-screening, and a range of other functions. This type of consumer-authorized data access and aggregation holds the promise of improved and innovative consumer financial products and services, enhanced control for consumers over their financial lives, and increased competition in the provision of financial services to consumers.

There are many significant consumer protection challenges to be considered—particularly with respect to data privacy and security—as these technologies and practices continue to develop. In part through a November 2016 public Request for Information, the Bureau is aware that a range of industry stakeholders are working, through a variety of individual arrangements as well as broader industry initiatives, on agreements, systems, and standards for data access, aggregation, use, redistribution, and disposal. The Bureau believes that consumer interests must be the priority of all stakeholders as the aggregation services-related market develops. A common understanding of consumer interests is essential so that effective consumer protections can be integrated consistently into this market.

As a result, the Bureau today is releasing a set of Consumer Protection Principles intended to reiterate the importance of consumer interests to all stakeholders in the developing market for services based on the consumer-authorized use of financial data. The Principles express the Bureau's vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value.

[1] 12 U.S.C. 5511(a).
[2] 12 U.S.C. 5511(b)(5).

The Bureau recognizes that many consumer protections apply to this market under existing statutes and regulations. These Principles are not intended to alter, interpret, or otherwise provide guidance on—although they may accord with—the scope of those existing protections. Thus, the Principles do not themselves establish binding requirements or obligations relevant to the Bureau's exercise of its rulemaking, supervisory, or enforcement authority. In addition, the Principles are not intended as a statement of the Bureau's future enforcement or supervisory priorities.

The Bureau will continue to monitor closely developments in this market. The Bureau will also continue to assess how the Principles set forth below may best be realized in the design and delivery of consumer financial products and services. The Bureau stands ready to facilitate constructive efforts or to take other appropriate action to protect consumers.

Consumer Protection Principles:
Consumer-Authorized Financial Data Sharing and Aggregation

Consumer-authorized access and use of consumer financial account data may enable the development of innovative and improved financial products and services, increase competition in financial markets, and empower consumers to take greater control of their financial lives. To accomplish these objectives, however, such access and use must be designed and implemented to serve and protect consumers. The Bureau intends for the following Consumer Protection Principles to help safeguard consumer interests as the consumer-authorized aggregation services market develops. The Principles are intended to be read together. They are not intended to alter, interpret, or otherwise provide guidance on—although they may accord with—existing statutes and regulations that apply in this market.

1) **Access**
Consumers are able, upon request, to obtain information about their ownership or use of a financial product or service from their product or service provider. Such information is made available in a timely manner. Consumers are generally able to authorize trusted third parties to obtain such information from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner.

Financial account agreements and terms support safe, consumer-authorized access, promote consumer interests, and do not seek to deter consumers from accessing or granting access to their account information. Access does not require consumers to share their account credentials with third parties.

2) **Data Scope and Usability**
Financial data subject to consumer and consumer-authorized access may include any transaction, series of transactions, or other aspect of consumer usage; the terms of any account, such as a fee schedule; realized consumer costs, such as fees or interest paid; and realized consumer benefits, such as interest earned or rewards. Information is made available in forms that are readily usable by consumers and consumer-authorized third parties. 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.

3) **Control and Informed Consent**
Consumers can enhance their financial lives when they control information regarding their accounts or use of financial services. Authorized terms of access, storage, use, and disposal are 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 include access frequency, data scope, and retention period. Consumers are not coerced into granting third-party access. Consumers understand data sharing revocation terms and can readily and simply revoke authorizations to access, use, or store data. Revocations are 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 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 are accessed, stored, used, and distributed securely. Consumer data are maintained in a manner and in formats that deter and protect against security breaches and prevent harm to consumers. Access credentials are similarly secured. 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. Security practices adapt effectively to new threats.

6) **Access Transparency**
Consumers are informed of, or can readily ascertain, which third parties that they have authorized are accessing or using information regarding the consumers' accounts or other consumer use of financial services. 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 is reasonably ascertainable to the consumer throughout the period that the data are accessed, used, or stored.

7) **Accuracy**
Consumers can expect the data they access or authorize others to access or use to be accurate and current. Consumers have reasonable means to dispute and resolve data inaccuracies, regardless of how or where inaccuracies arise.

8) **Ability to Dispute and Resolve Unauthorized Access**
Consumers 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 are not required to identify the party or parties who gained or enabled unauthorized access to receive appropriate remediation. Parties responsible for unauthorized access are held accountable for the consequences of such access.

9) **Efficient and Effective Accountability Mechanisms**
The goals and incentives of parties that grant access to, access, use, store, redistribute, and dispose of consumer data align to enable safe consumer access and deter misuse. Commercial participants are accountable for the risks, harms, and costs they introduce to consumers. Commercial participants are likewise incentivized and empowered effectively to 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.