October 18, 2017

Consumer-authorized financial data sharing and aggregation

Stakeholder insights that inform the Consumer Protection Principles

Introduction

Consumer-authorized access to consumer financial account data in electronic form may enable consumer-friendly innovation in financial services. Companies that consumers authorize to access their digital financial records can aggregate and use those records to offer new products and services aimed at making it easier, cheaper, or more efficient for consumers to manage their financial lives. At the same time, this kind of expanded access to consumer financial records raises a number of concerns, particularly with respect to data security, privacy, and unauthorized access.

The Consumer Financial Protection Bureau (CFPB or Bureau) has developed a set of Consumer Protection Principles for market participants to consider as this "aggregation services" market continues to develop. The Principles are presented in a separate document. The present document highlights feedback that the Bureau received from its outreach that supports or discusses concepts addressed in the Principles. This document is not, nor is it intended to be, a complete summary of the feedback that the Bureau has received. Nonetheless, the full range of stakeholder feedback that the Bureau has received to date informs the Bureau's ongoing work in this area.

The Bureau is committed to monitoring the aggregation services market and ensuring consumer protection and safety. In November 2016, the Bureau published a Request for Information (RFI)

to inquire into issues regarding the aggregation services market.[1] In addition, the Bureau has met and continues to meet with various stakeholders to understand the benefits that consumers may receive and the risks that consumers may face when they access and share their financial records with third parties.

Entities involved in providing aggregation services include "aggregators," which are companies that collect information from other providers; "account data users" that use aggregators to offer various (often digital) consumer financial products and services; and "account data holders," oftentimes banks or credit unions, that hold account and other data about consumers. Some entities may fill more than one of these roles. The RFI and related outreach efforts have elicited comments and feedback from a broad range of stakeholders, including large and small account data holders, their trade associations, aggregators, account data users, individual consumers, and consumer advocates.[2]

The feedback received by the Bureau acknowledges consistently the importance of ensuring consumer protections for safe access to, and controlled use of, consumer financial data by consumers and third parties. While few, if any, individual stakeholders enumerate all of the consumer protection concerns presented in the Bureau's Principles, stakeholders generally recognize the need for market participants to work to develop data access and use practices that are based on a shared set of standards and expectations and that address consumer protection.

Views vary regarding how best to realize these consumer protections. Some of the varying views are described below. With respect to the Bureau's role, some stakeholders ask the Bureau to assume a substantive and formal role in moving the aggregation services market forward. These stakeholders generally take the view that CFPB regulatory action, which could include a

[1] Request for Information Regarding Consumer Access to Financial Records, 81 FR 83806 (Nov. 22, 2016).

[2] A full set of the comments the Bureau received in response to the RFI can be found at https://www.regulations.gov/docket?D=CFPB-2016-0048.

rulemaking that involves Section 1033 of the Dodd-Frank Act[3], clarification of existing regulations, or expanding CFPB supervisory authority to include aggregators and account data users by means of "larger participant" rulemakings, may be necessary to ensure consumers are protected as the market continues to develop. Others assert that market participants should be entrusted to develop solutions, such as data or security standards, that protect consumer interests with minimal Bureau involvement, if any at all. A third and final group of stakeholders state that the Bureau should play some role in facilitating industry's development of data sharing practices but should not initiate formal regulatory action, or at least not unless and until industry-developed mechanisms have had a chance to succeed. A few stakeholders that advocate for limited Bureau involvement and against rulemaking appear to do so in part because of concerns that any data sharing requirements imposed by the Bureau could impose excessive burdens on small market participants, such as community banks and smaller credit unions.

In developing these Principles, the Bureau has taken into account the comments received in response to the RFI as well as other stakeholder feedback. The Bureau has organized this document to highlight insights gained from that feedback under the following subject categories:

- Access;
- Data scope and usability;
- Control and informed consent;
- Authorizing payments;
- Security;

[3] Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) provides for consumer rights to access information about their financial accounts. Specifically, Section 1033(a) requires 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." Section 1033 further provides that the information must be in an electronic form usable by the consumer, although it does not impose any duty to maintain or keep any information about a consumer. Additionally, Section 1033 does not apply to information that the consumer financial account data holder cannot "retrieve in the ordinary course of its business with respect to that information."

- Transparency of access;
- Accuracy;
- Ability to dispute and resolve unauthorized access; and,
- Efficient and effective accountability mechanisms.

The Bureau continues to engage with stakeholders to help it determine the best approach for ensuring appropriate consumer protections for users of aggregation services. Market participants and other stakeholders that want to engage with the Bureau on these issues may contact consumerdataaccess@cfpb.gov.

1. Access

Stakeholders generally agree that consumers should have secure access to their financial data, and that such access may benefit consumers when the data are used in conjunction with certain products and services. Consumer-authorized access enables account data users to provide consumers with a variety of products and services, including personal finance management (PFM) tools, saving and budgeting tools, debt repayment assistance, financial planning, and identity verification and authentication. Some stakeholders, particularly those that offer these products, posit that many of these products provide consumers greater insight into their financial lives as well as allow for more informed financial decision making and enhanced consumer control over their finances. Furthermore, some stakeholders—mostly aggregators and account data users—note that when consumers can authorize third parties to access data safely and securely in digital formats, market competition for consumer services and innovation increase, and consumers further benefit.

Further, many account data holders acknowledge that they could face consumer dissatisfaction and competitive disadvantage by preventing consumer-authorized access to third parties. However, there is not universal agreement regarding consumers' rights to grant access to their financial information to aggregators and account data users.

A number of stakeholders, representing primarily account data holders, question the applicability of Section 1033 to consumer-authorized data access (as opposed to consumer's direct access) and thus encourage the Bureau to not embark on a Section 1033 rulemaking in this area. On the other hand, aggregators, account data users, and consumer advocates generally

argue that Section 1033 applies to consumer-authorized data access, although not all of these commenters urge the Bureau to conduct a Section 1033 rulemaking at this time.

2. Data scope and usability

As noted above, there is general agreement that consumers should have secure access to their financial data. There is some disagreement, however, as to which types of data consumers should be able to access and share with aggregators and account data users. Aggregators and account data users generally allege the importance of consumers having access to a diverse and unlimited array of consumer data to maximize the effectiveness and usability of the various products and services that rely on aggregated consumer data. Account data holders express concerns to the Bureau about sharing certain types of data, particularly data they find extraneous to account data user needs and data that might be used to reverse engineer proprietary models.

Some aggregators and account data users raise concerns that account data holders may restrict or control, in an unreasonable and anti-competitive manner, the type of data that they permit consumers to authorize third parties to access. These stakeholders assert that such practices could limit the usability of consumer financial products and services that rely on aggregated consumer data. Conversely, account data holders and consumer advocates express concerns that aggregators may be accessing more data than necessary to deliver the consumer financial products and services that consumers request. Risks that these stakeholders identify include identify theft, fraud, and unauthorized use of consumer account credentials. Account data holders also express concerns that, if a breach or hack occurs as a result of consumer-authorized data access, they could risk exposure to regulatory action and private litigation or reputation and revenue loss. To limit these risks, stakeholders suggest that the Bureau could limit access to and the use of consumer financial data to the express purpose for which the consumer has authorized that access.

3. Control and informed consent

Stakeholders emphasize that consumers should retain control over access to their financial data (*i.e.*, consumers should be free to authorize who does and does not have access to their data and to revoke such authorizations at will and with reasonable specification). Further, a number of

stakeholders appear to agree generally that consumers should understand the costs, benefits, and risks they may realize when they authorize third parties to access their data.

Many stakeholders express concern that consumers may not read or understand the terms presented in disclosures when they authorize third-party access to their data. As a result, some stakeholders assert that this might impede the ability of consumers to be truly informed about how often their data are being accessed, how long their data are being retained, whether the data presented to them are accurate or complete, with whom their data are being shared, and the risks associated with sharing their data and account credentials.

Some account data holders suggest that some consumer-authorized sharing arrangements afford consumers inadequate mechanisms to limit or revoke access by not making these functions readily available. In addition, a variety of stakeholders acknowledge that consumers may have particular challenges in managing multiple sharing arrangements. As an example, they point how consumer comprehension and control are impeded by inconsistent practices and agreement terms related to how data are accessed, used, and stored.

Proposed solutions that could address weaknesses around consumer consent and control in the market fall into two broad buckets. First, account data holders and consumer advocates assert that effective disclosures could help ensure consumers have the necessary information to make informed choices about how and with whom they share data. Second, account data holders and aggregator stakeholders suggest that consumers should be given the opportunity to provide explicit consent for data access and the ability to confirm, revoke, or modify access easily once it is granted.

4. Authorizing payments

Some account data users provide products and services that initiate funds transfers out of consumers' bank accounts on consumers' behalves. (For example, a third-party bill payment platform.) Other account data users may not initiate consumer funds transfers but nonetheless may collect, use, and retain credentials or account information that can be used to initiate payments. Stakeholders raise questions regarding whether and when a consumer's provision of account credentials to a third party means that the consumer has thereby authorized that party to initiate payments. They also raise concerns about what consumers may (or may not) understand about the authorizations they are providing. Aggregators and account data users

generally recognize that there is heightened sensitivity around consumers sharing or authorizing access to account credentials that could be used to initiate electronic funds transfers.

Some aggregators and account data users indicate that they support methods by which consumers can authorize access without providing general account credentials to the aggregator or account data user. Stakeholders, including aggregators and account data users, state that this approach can enhance consumer control and help limit the risk that payments are made from a consumer's account without that consumer's actual authorization.

5. Security

Stakeholders generally agree that consumer data security must be a core and shared focus for and between all participants in the data aggregation services market. Account data holders and trade associations representing them emphasize the importance they place on safeguarding consumer data in the context of consumers authorizing broader data access. Similarly, data aggregators and account data users stress the importance of protecting the security and integrity of these data. Stakeholders also generally agree that consumers should not have to sacrifice data security or accessibility to realize the benefits of the aggregation services market.

In addition, as referenced above, many stakeholders agree that viable forms of access exist that are more secure than those that require consumers to share account credentials with third parties. And many stakeholders, including account data holders, aggregators, and account data users, discuss in detail the various technologies, processes, and mechanisms they currently implement to safeguard consumer data that they access, use, or distribute.

However, despite the availability of such solutions and broad stakeholder agreement that security is paramount, some—particularly account data holders and consumer advocates—stress that any time consumer data move from an account data holder to an aggregator or account data user, the security of that data is put at risk. These stakeholders emphasize that all parties involved in data aggregation are or should be responsible for ensuring that consumers' data are accessed, stored, used, distributed, and disposed of securely. They raise concerns that not all participants in the data sharing market are currently held to the same data security standards and regulatory requirements and oversight. Additionally, they assert that some market participants may not adequately protect consumer data, particularly because, in their view, these participants underinvest in security or use less secure technologies. On the other hand,

aggregators, account data users, and consumer advocates are concerned that account data holders may use security concerns as a pretext to limit or block data sharing.

There are also varying views about how to establish a secure data sharing ecosystem, including what role, if any, the government, in general, and the Bureau, in particular, should play. Aggregators and account data users tend to believe that current levels of oversight, combined with existing market incentives, are adequate to establish such an ecosystem. A number of aggregators and account data users further note that they are already subject to rules concerning information security. On the other hand, account data holders and consumer advocates suggest that the Bureau take steps to extend oversight formally to aggregators and account data users, through, for instance, its supervisory authority. Relatedly, consumer advocates tell the Bureau that they believe the Bureau has regulatory and enforcement jurisdiction over aggregators and account data users.

Finally, many stakeholders suggest specific mechanisms, processes, and technologies that they argue should be implemented industry-wide to ensure safe and secure data sharing. These include permitting only "read only" access to financial data, which could prevent third parties from initiating unauthorized funds transfers during aggregation access; the tokenization of account credentials to eliminate the need to share account credentials with third parties; and the use of application programming interfaces and other technologies to enable more secure transmission of consumer data.

6. Access transparency

Broadly, stakeholders acknowledge that consumers' understanding of their authorized sharing relationships varies. Stakeholders, including aggregators and account data users, further acknowledge that there is wide disparity within the current market regarding what consumer data are accessed, how often data are accessed, for what purposes data are used, and for how long data are stored.

Consequently, many stakeholders stress the need for "access transparency." More specifically, many, including account data holders and consumer advocates, assert that when a consumer authorizes aggregators and account data users to access their financial data, the consumer should understand what data are being accessed, how long the data will be held, and how the data will be used throughout the customer relationship.

To enable such access transparency, consumer advocates promote the provision of consumer tools, either from account data holders or account data users, to help consumers understand how and why their information is being accessed. Account data holders also generally argue that consumers should have access to such tools, and at least some have proposed creating dashboards for their customers to enable consumers to monitor the sharing arrangements they have authorized. Such dashboards could enhance both transparency and consumer control by allowing consumers to readily view, modify, and revoke access to third parties.

Some account data holders assert that it is important that they know which account data users and other third parties could obtain their customers' data and for what purposes. These account data holders posit that such information would allow them to vet third parties to whom consumers authorize access, suspend or terminate sharing arrangements if third parties breach the sharing agreement or fail to meet security standards, comply with their regulatory obligations, and better protect consumers. At least one stakeholder suggests the idea of a regulator or governance body that could assess and credential companies as safe and trusted third parties.

7. Accuracy

Stakeholders generally agree that information consumers authorize third parties to access from account data holders should be accurate, reliable, and timely. However, not all stakeholders agree upon the extent to which consumers are provided with timely and accurate information in the current aggregation services market.

Many stakeholders acknowledge that screen scraping algorithms may be at greater risk of missing or misinterpreting data fields than sharing processes in which account data holders transmit data to account data users or aggregators through direct data feeds. At the same time, some account aggregators and account data users have raised concerns that account data holders may demand sharing agreements that do not rely upon sharing of credentials and provide direct data feeds, but that would also restrict the frequency or timing of when authorized aggregators could access consumer data. These stakeholders assert that such agreements could hinder account data users' ability to provide consumers with timely and accurate information, and hence limit their ability to deliver useful products and services to consumers. Lastly, at least one stakeholder has raised the need for mechanisms for consumers to report and resolve inaccurate or incomplete data.

8. Ability to dispute and resolve unauthorized access

Stakeholders generally acknowledge that there is some risk of unauthorized access to consumers' underlying financial services account when consumers share their account information with third parties. Unauthorized access can lead to unauthorized debits from consumers' deposit accounts (or unauthorized charges on their credit accounts). Stakeholders also generally agree that consumers may lack clear mechanisms for reporting, disputing, and resolving transactions that arise due to unauthorized access related to data aggregation products.

There are varying views on how consumers should be protected in the event that unauthorized access occurs. Account data holders, aggregators, and account data users suggest that consumers may not always be protected by provisions in the Electronic Fund Transfer Act (EFTA) and its implementing rule, Regulation E, that apply to unauthorized debits when consumers share their account information. Consumer advocates, on the other hand, generally maintain that consumers retain their rights and the ability to dispute and resolve unauthorized charges pursuant to EFTA and Regulation E if unauthorized debits are made from consumers' accounts when they use data aggregation services. Given this disagreement, some stakeholders urge the Bureau to clarify how the relevant EFTA and Regulation E provisions apply to consumers when they are using aggregation services.

9. Efficient and effective accountability mechanisms

Stakeholders agree that consumer protection is a shared responsibility in the aggregation services market. They provide diverse recommendations to maintain and enhance consumer protection in this market. In particular, account data holders, aggregators, and account data users describe to the Bureau the ways in which they are currently collaborating with each other to develop practices, standards, and rules that prioritize consumers' interests. They also discuss how they believe these mechanisms could be adopted and enforced industry wide. Aggregators and account data holders highlight the various accountability mechanisms they are required to follow or currently voluntarily implement. These mechanisms include, but are not limited to, data security and privacy standards, audits or vetting of entities that participate in the data sharing ecosystem, and indemnification agreements and insurance to compensate consumers in the event of losses.

Despite these private, bilateral, and multilateral industry efforts, stakeholders' opinions vary regarding the effectiveness of industry self-regulation. As noted above, some stakeholders ask the Bureau to assume a formal role in ensuring consumer safety and viability throughout the aggregation services market. Others state that market participants could protect consumer interests without Bureau involvement, and still some others argue that the Bureau should play some role in facilitating market development, but not assume a formal role.