ConsumersUnion®
POLICY & ACTION FROM CONSUMER REPORTS

February 21, 2017

Monica Jackson
Office of the Executive Secretary
Consumer Financial Protection Bureau
1700 G Street, NW
Washington DC 205552

Re: Docket No. CFPB-2016-0048
Request for Information Regarding Consumer Access to Financial Records

Dear Ms. Jackson:

Consumers Union, the policy and mobilization arm of Consumer Reports,[1] appreciates this opportunity to comment on the Bureau's Request for Information (RFI) Regarding Consumer Access to Financial Records.

Our comments below focus on the benefits consumers experience thanks to the ability to access their financial records and make use of third party financial management tools. Although these products can enable consumers to more effectively manage their personal finances, the potential benefits these services may offer in some cases may be undercut by gaps in consumer protections. The uneven consumer protection landscape of third-party financial management tools may leave some consumers, especially economically vulnerable consumers, at a greater risk of fraud or loss.

For these reasons, although we urge the Bureau to help consumers realize these benefits through the use of these tools, the Bureau should use its authority, as well as work with Congress and other relevant agencies, to ensure that consumers receive baseline protections when accessing and using third-party financial management services. Since these products depend on consumers granting permission to these companies to access their financial records, consumers should have the ability to choose and assess these diverse products with confidence and the assurance that they are not putting their data at risk.

We include recommendations for the Bureau, as well as other regulators, lawmakers, and service providers to ensure that consumers using these new technologies are protected and consumers have adequate control over their personal financial data.

Accordingly, our response to particular questions posed by the Bureau:

[1] Consumers Union is the policy and mobilization arm of Consumer Reports. Consumers Union is an expert,

1. What types of products and services are currently made available to consumers that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data? What benefits do consumers realize as a result?

Consumer-permissioned access to financial records enables individuals to manage their investments, payroll, invoicing, personal financial management, accounting, payments/funds transfer, lending, saving, peer-to-peer payments, expense management, and charitable savings. These tools allow consumers to effectively save, pay off debts, manage their small business, and pay peers for small transactions, among other uses.

Although some consumers continue to prefer a pen-and-paper approach to their personal financial management, for a growing number of consumers, automation is the key to effectively managing their finances. Despite concerns about hacking, consumers desire access to the tools financial services technology provides. Access to personal financial management products is especially important to consumers that are under-supported or underserved by traditional financial management methods. Younger consumers and lower-income consumers have the ability to grow and manage their wealth through new tools provided by account aggregators. Account aggregation also allows advisers to have a full view of clients' accounts.[2]

4. To provide or assess eligibility for these products and services, what kinds of non-financial consumer account data are being accessed by parties that also access consumer financial account data? By what means, under what terms, and how often? How long is accessed data stored by permissioned parties or account aggregators?

These financial products and services should not have access to non-financial consumer account data that is not clearly necessary to the provision of those services, unless there is a clear and defined need that is expressed to the user. Consumers can be wrongly assessed by the use of non-financial consumer data in order to determine whether to provide access to lending, payment, or transaction tools. The access to non-financial consumer data can be compared to the use of non-driving factors that are used to calculate insurance risk. Using non-driving factors to inform insurance pricing has the potential to arbitrarily and unfairly discriminate against some consumers. Similarly, the use of data that is unrelated to a consumer's financial records and payment history could lead to unfair bias against some consumers. Therefore, access to non-financial consumer data should be closely regulated and limited.

14. When consumers permit access to their financial account data, what do they understand about: what data are accessed; how often they are accessed; for what purposes the data are used; whether the permissioned party or account aggregator continues to access, store or use such data after the consumer ceases to use the product or service for which the permissioned data use was intended by the consumer; and with which entities a permissioned party or account aggregator shares the data and on what terms and conditions? What drives or impacts their level of understanding? What impact does their level of understanding have on consumers and on other parties, including on consumers' willingness to permit access?

[2] Veronica Dagher, *Consumers' Finance Data Still Flows at Aggregation Services for Financial Advisers*, WALL STREET J. (Nov. 11, 2015), https://www.wsj.com/articles/consumers-finance-data-still-flows-at-aggregation-services-for-financial-advisers-1447286131.

15. To what extent are consumers able to control how data is used by permissioned parties or account aggregators that obtain their data via consumer-permissioned access? Are consumers able to control what data are accessed, how often they are accessed, for what purposes and for how long the data are used, and with which entities, if any, a permissioned party or account aggregator may share the data and on what terms and conditions? Are they able to request that permissioned parties, account aggregators, or other users delete such data? Is such data otherwise deleted and, if so, when and by what means? To what extent are consumers consenting to permissioned party and account aggregator practices with respect to access, use and sharing of consumer financial data?

What do consumers understand about what financial data is collected?

(Questions 14 and 15)

A reasonable consumer may expect that companies will collect financial data as necessary for everyday business purposes or identity verification. However, a brief look at the privacy policies of three industry leaders reveals that consumers are likely ignorant of the full range of data that companies access, as each company has unique definitions of personal data.

For example, one company requires broad access to credit score and credit history, bill and payment information, and any third party data synced with the user's account.[3] Another company does not collect credit score information, but requires specific credit card and debit card information, including card number, expiration date, billing address and other payment related information.[4] Finally, a third company collects personal information that consumers provide, but does not explicitly state which information is required for which purposes.[5] The result of these separate definitions is that consumers cannot have a general understanding of why their information is being accessed.

Consumers should have access to tools, either from their banking institution or the third party financial management companies, to understand why their information is being accessed.

What data may consumers limit?

(Questions 14 and 15)

Generally, consumers can view the ability to limit data collection in three categories: data collection that may be limited by opting out, data collection that consumers may request that the company limit, and data collection that consumers cannot limit. Consumers may opt out of sharing their information with affiliates about their creditworthiness. However, the default practice is to begin sharing data until consumers act to opt out, putting the burden on consumers to take action.

[3] Mint, https://www.mint.com/privacy.
[4] BillGuard, https://www.billguard.com/daily/privacy.
[5] PowerWallet, https://www.powerwallet.com/app/privacy.

For example, Mint users have a right to opt out of sharing personal creditworthiness data with affiliates (this is indicated by a chart on their Privacy Statement).[6] However, Mint users cannot opt out of data sharing with affiliates for business purposes. The terms state that users can email the company to request a limitation of sharing of personal information (but does not say whether the company must honor those requests).[7] Consumers may broadly request to limit the collection of personal information by contacting the company, though it is unclear what data the consumer may request to opt out of, and whether the company must honor those requests.

Further, it is unclear whether consumers are aware that they are required to do so by phone or email. Some companies explicitly provide that consumers may not limit access to other data. For example, the consumer may restrict affiliates from *using* personal data to market to that consumer; however, the consumer may not be permitted to prevent affiliates from *accessing* personal data for marketing purposes.

In other words, consumers may have the option to request limiting the sharing of some types of personal data, but do not have the ability to opt out of affiliates accessing many types of personal data.The only constant control consumers have is over geo-location data, and this control stems from a consumers' ability to turn off location access from their device rather than from the app itself. Accordingly, consumers should have better controls to limit access to their personal data.

What do consumers understand about a permissioned party's access to consumer data?

(Questions 14 and 15)

Generally, companies provide that they will make commercially reasonable efforts to delete data. However, there is no additional guidance on when a consumer can find out whether their data has been deleted. Therefore, consumers cannot have a quantifiable expectation as to when a company stops retaining and sharing personal data.

To further complicate matters, some companies provide that personal information will be retained as long as necessary, and as permitted by applicable law. This essentially means that such companies will likely be able to err on the side of retaining information rather than removing it.

Third party financial management companies should limit the amount of data they retain on consumers, and consumers should be informed about company data retention policies.

16. Do consumer financial account providers vet account aggregators or permissioned parties before providing data to them? Do consumer financial account providers perform any ongoing vetting of account aggregator or permissioned parties? If so, for what purposes and using what procedures? What are the associated impacts to consumers and to other parties?

[6] Mint, https://www.mint.com/privacy.
[7] *Id.*

We urge the Bureau to use this RFI as an opportunity to assess the market and support financial account providers, account aggregators, and permissioned parties that do vet a third party before allowing information to be accessed. We urge the Bureau to reject traditional banking institutions who assert that consumers lose their protections under Regulation E[8] against unauthorized charges if they use a data access service. Providing access via login information to a service for the purpose of helping the consumer view financial accounts in one place should not be treated as equivalent to a hacker gaining access to these financial accounts.

Conclusion

Third-party financial management tools have the ability to provide consumers with more convenient and effective ways to manage their personal finances. However, these products need to have robust protections and effective consumer controls in order to avoid consumer mistrust and unauthorized access to sensitive financial data. Lawmakers, regulators, and industry actors need to act to ensure that adequate consumer protections for users are incorporated into the design of these products from the outset. We look forward to working with the Bureau to ensure that these financial management tools provide consumers with all possible benefits while also sufficiently protecting consumer financial data.

Respectfully submitted,

Katie McInnis
Staff Attorney

George Slover
Senior Policy Counsel

Karim Salamah
Legal Fellow

Christina Tetreault
Staff Attorney
Consumers Union

[8] 12 C.F.R. § 1005.