NCLC®
NATIONAL CONSUMER LAW CENTER®
Advancing Fairness in the Marketplace for All

BOSTON HEADQUARTERS
7 Winthrop Square, Boston, MA 02110-1245
Phone: 617-542-8010 • Fax: 617-542-8028

WASHINGTON OFFICE
1001 Connecticut Avenue NW, Suite 510, Washington, DC 20036
Phone: 202-452-6252 • Fax: 202-296-4062

www.nclc.org

February 21, 2017

Via regulations.gov
Monica Jackson
Office of the Executive Secretary
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Comments in Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048

Thank you for the opportunity to respond to the Consumer Financial Protection Bureau's (CFPB) Request for Information Regarding Consumer Access to Financial Records (RFI). We are pleased that the Bureau is giving attention to consumers' important rights under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) to access their own financial account and account-related data in usable electronic form.

These comments address these key points:

1. Consumers can benefit from third-party services that access their financial account data, and the CFPB should prevent financial institutions from blocking access to that data for the purpose of stifling competition.

2. The CFPB should take action to stop financial institutions from falsely telling consumers that they lose protection against unauthorized charges if they permit a third party to access their account data.

3. Though their motives are mixed, financial institutions are rightly concerned about security issues. The CFPB should work with financial institutions, data aggregators and intermediaries to facilitate methods of account data sharing that avoid security risks.

4. Third parties that access account data can create serious privacy issues that consumers are not aware of and have difficulty controlling. The CFPB should work to limit these privacy risks.

5. Consumers should be able to access and store their data in order to move their account.

6. The CFPB should supervise the larger data aggregators and intermediaries.

7. The CFPB should use its authority under section 1033 of the Dodd-Frank Act to give consumers a right to access the actual consumer report or risk score used to assess the consumer.

Providing access to account data requires a nuanced approach. Important benefits can come from accessing one's own account data. But consumers cannot be expected to understand the complex risks that come from sharing that data. The CFPB can play a key role to facilitate the benefits and minimize the risks.

1. Consumers can benefit from accessing their financial account data, and the CFPB should prevent financial institutions from blocking access to that data for the purpose of stifling competition.

A growing number of mobile apps and internet services are offering services to consumers that utilize information about consumers' financial accounts. These providers can offer useful and innovative services that improve consumers' lives in a variety of ways. Services can help consumers manage their financial lives by providing a full picture of all of their financial accounts in one place. Aggregated information, visuals, alerts and other tools can help consumers budget, limit spending, and manage their finances. Services may alert consumers to unwanted fees, help them avoid overdrafts, and provide reminders and tools to pay bills easily and on time. Apps draw on lessons from behavioral economics to help people save and avoid overspending.

Access to account information can drive many useful and innovative services that consumers do not receive directly from the provider of the account. These services can enhance those that financial institutions provide directly. These innovations can also spur greater competition for financial institutions to improve their own services.

Financial institutions may not offer the same features that third-party providers do for a variety of reasons. Consolidation of information from several accounts may be necessary. The idea for the feature may first arise in fintech startups. Financial institutions may be slower to evolve, adding in new services cautiously. And in some cases – as in the case of overdraft fees – financial institutions' incentives may be misaligned with their customers' goals, as they may prefer that their customers continue incurring unwanted fees.

Account-holding institutions have reasons not to want their customers to be able to provide third parties with access to account information. Even if the third-party service is not inconsistent with the financial institution's profit model, banks want to control access to their customer and inhibit competition. They want to build brand loyalty, to have services come through them, and do not want startups offering competing services. This is especially true as a broader array of companies offer financial services that previously were offered by banks and credit unions alone.

Some financial institutions have taken steps to inhibit consumers from accessing their own data through third-party services. Banks have given consumers alarming and deceptive warnings about liability risks and have refused to cooperate with third-party services.

As discussed below, security can be a legitimate concern. But anti-competitive motives should never be allowed to interfere with consumers' ability to access their own data safely.

Section 1033 of the Dodd-Frank Act states 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 such person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, or series of transactions, to the account including costs, charges, and usage data." The CFPB should implement that section by preventing financial institutions from unduly inhibiting consumers' access to their own data.

2. The CFPB should take action to stop financial institutions from falsely telling consumers that they could lose protection against unauthorized charges if they permit a third party to access their data.

Some financial institutions take the position that consumers lose their dispute rights and liability protection under Regulation E if they give a third party permission to access their account and unauthorized charges result. That is incorrect. The CFPB should take action to stop financial institutions from misrepresenting consumers' liability rights in order to discourage use of competing services. (At the same time, as discussed in the next section, the CFPB should facilitate safe methods of data sharing.)

For example, Chase has used scare tactics to try to persuade consumers not to use services like Intuit's Mint, a data aggregation service that enables consumers to view and manage all of their financial accounts in one place.[1] The CEO of Chase, for example, said:

When customers give out their bank passcode, they may not realize that if a rogue employee at an aggregator uses this passcode to steal money from the customer's account, the customer, not the bank, is responsible for any loss.[2]

Similarly, the terms and conditions section of the Chase bill payment and transfer services agreement states:

You are responsible for all transfers and payments that are authorized using your Online Service Password. If you permit other persons to use the Online Service or your Password, you are responsible for any transactions they authorize. NOTE: ACCOUNT ACCESS THROUGH THE ONLINE SERVICE IS SEPARATE AND DISTINCT FROM YOUR EXISTING SIGNATURE ARRANGEMENTS FOR YOUR ACCOUNTS. THEREFORE, WHEN YOU GIVE AN INDIVIDUAL THE AUTHORITY TO ACCESS ACCOUNTS THROUGH THE ONLINE SERVICE, THAT INDIVIDUAL MAY HAVE ACCESS TO ONE OR MORE ACCOUNTS TO WHICH THAT INDIVIDUAL WOULD NOT OTHERWISE HAVE SIGNATURE ACCESS. YOU ASSUME THE ENTIRE RISK FOR THE FRAUDULENT, UNAUTHORIZED OR OTHERWISE IMPROPER USE OF YOUR PASSWORD. WE SHALL BE ENTITLED TO RELY ON THE GENUINENESS AND AUTHORITY OF ALL INSTRUCTIONS RECEIVED BY US WHEN ACCOMPANIED BY SUCH PASSWORD, AND TO ACT ON SUCH INSTRUCTIONS.[3]

---

[1] Liz Weston, "Why banks want you to drop Mint, other 'aggregators'", Reuter (Nov. 9, 2015), http://www.reuters.com/article/us-column-weston-banks-idUSKCN0SY2GC20151109.

[2] Letter from Jamie Dimon, Chairman and Chief Executive Officer, JP Morgan Chase, to Shareholders at 21 (Apr. 6, 2016), https://www.jpmorganchase.com/corporate/investor-relations/document/ar2015-ceolettershareholders.pdf. The terms and condition of one Chase account are similar though perhaps slightly narrower: "If you permit other persons to use the Bill Payment and Transfer Service or your Password, you are responsible for any transactions they authorize from your accounts."

[3] https://www.chase.com/index.jsp?pg_name=ccpmapp/shared/help/page/BillPay_LA_cbmc.

These are inaccurate statements of consumers' Regulation E rights and responsibilities. Regulation E rights are not waivable and financial institutions may not change them by contract.[4]

Chase is likely relying on this exception to consumers' protection from unauthorized charges:

The term [unauthorized transaction] does not include an electronic fund transfer initiated:

> 1. By a person who was furnished the access device to the consumer's account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized.[5]

This provision is intended to address a situation such as when a parent provides a debit card and PIN to child or spouse and the child or spouse misuses it to make purchases that the parent did not intend. In that situation, unless the parent has notified the financial institution that use of the debit card is no longer authorized, the parent is still responsible.

But this exception to the Regulation E liability protection does not deprive consumers of error resolution or liability protection when they provide account credentials to third-party services that access account data in the course of providing services to the consumer. Even assuming that a username and password combination is an "access device" and was the device used to make the transfer,[6] the "person" that was furnished the access device is the third-party service, such as Intuit, not a rogue employee. The consumer did not furnish the access device to a rogue employee.

The application of the Regulation E exception is even more strained if Mint, for example, had a data breach and the account credentials were stolen. The thief certainly was not furnished the access device by the consumer. Any transfers made by the thief would be unauthorized and the consumer would have full regulation E protection. When Chase claims that the consumer assumes "the entire risk for the fraudulent, unauthorized or otherwise improper use" of the password, and that Chase is "entitled to rely on the genuineness and authority" of all instructions when accompanied by the password, it is going far beyond the limited exception.

Chase's position that consumers bear the sole risk of loss when instructions are accompanied by use of the password would deny consumers their Regulation E rights if their username and password were in their wallet and were stolen. Yet even if the consumer is negligent, negligence does not revoke liability protection.[7]

Moreover, if the consumer faces unauthorized charges, tracing the source of the problem is not an easy matter. How is either the consumer or the bank to know that it was a rogue employee at the data aggregator rather than a rogue employee at the bank? Even if there has been a data breach at the data aggregator, many banks – including Chase – have suffered their own data breaches. Which one was the source of the problem?

---

[4] Reg. E, § 1005.6(b)(6); Reg. E, Official Interpretations § 1005.6(b)-3;NCLC, Consumer Banking & Payments Law § 5.1.2a, updated online at library.nclc.org.

[5] 12 C.F.R. §1005.2(m).

[6] A person who logs in to the account, obtains the account number, and initiates an ACH debit transaction using the account number and bank routing number is using an access device that was not furnished by the consumer.

[7] Reg. E, Official Interpretations § 1005.6(b)-2.

Consumers need a clear single source of error resolution if they have been the subject of unauthorized charges. That source, under the mandate of Regulation E, is the account-holding institution.

While Chase has worked out an arrangement with Intuit for Mint,[8] its erroneous claims about liability protection could still inhibit consumers from using other services. The CFPB should take action against Chase and any other financial institutions making similar statements or putting similar language in their account agreement inappropriately revoking Regulation E rights.

While the account-holding institution is responsible to compensate the consumer for unauthorized charges, certainly that institution should in turn be able to recover from a third party that is the source of the problem. We also agree that all parties should work to find secure ways of sharing data, as discussed in the next section.

3. The CFPB should facilitate methods of account data sharing that avoid security risks.

While financial institutions that resist data sharing are sometimes motivated by anti-competitive reasons, there also can be real security concerns. These concerns arise for a number of reasons.

Today, many third-party services rely on consumers' giving them usernames and login information. Providing that type of direct login information poses obvious risks. First, the third party itself, or its employees, could abuse the access. Second, if not held securely, the information could be the target of a data breach and stolen by identity thieves.

As discussed in the previous section, we disagree with any claim that consumers lose Regulation E rights when their login credentials are misused for purposes not authorized. At times, purported security concerns about third parties that have robust security controls may be masking anti-competitive motives.

But we agree that financial institutions have legitimate security concerns about the sharing of account credentials and reasons to want to inhibit account access by parties that pose undue risks. Consumers have little capacity to evaluate the trustworthiness, security protocols, motives or activities of companies that offer services based on account data. It can be in the consumer's interest for a financial institution to inhibit access by companies that pose undue risks to the consumer.

Some services may rely on screen-scraping capacities and application program interfaces (APIs) that can access information without the ability to transfer funds, change passwords or addresses, or otherwise take any actions with respect to the account. While less problematic than direct access, the information that can viewed may still be sensitive. Account numbers, direct deposit information, and other information could be misused in the wrong hands.

The issues involved are complicated and cannot be solved simply by consumer disclosures. Consumers do not have the ability to determine if the manner of accessing their data is safe, or if the company is using secure measures to hold the data.

[8] Press Release, Intuit, "Chase, Intuit to Give Customers Greater Control of Their Information" (Jan. 25, 2017), https://www.intuit.com/company/press-room/press-releases/2017/Chase-Intuit-to-Give-Customers-Greater-Control-of-Their-Information/.

The CFPB should work with the other bank regulators, the FTC, financial institutions, data aggregators, intermediaries and other parties to address both issues – how data is shared, and what security must be in place for companies that access account data – in order to protect both consumers and institutions from the risks of inappropriate access and use of that data.

4. Consumers need more protection from the privacy risks of account data access.

Beyond security risks, consumers also face privacy risks when they provide access to their account data. Consumers may believe that they are providing access only for purposes of a narrow range of transactions or services. But the third party can gain access to a wealth of information about the consumers' income, purchases, spending patterns and a variety of other sensitive personal information. Some services harvest this information for marketing purposes and even at times may reserve the right to share it with other parties that the consumer does not contemplate.

The vague, long, fine print privacy policies that consumers receive do not give them any real idea of how their information may be used. Consumers also may have used a service once or twice to try it out and long forgotten about it, not realizing their information is still being collected and potentially disseminated. While consumers have the right to limit data sharing with unrelated third parties, they are often unaware of those rights, and may have difficulty knowing how to change their preferences.

While privacy issues plague a wide variety of financial and nonfinancial services, they are particularly acute given the sensitive information that may be obtained through access to a financial account. We urge the CFPB to work with the FTC and, if necessary, Congress to protect consumers' privacy and make it easier for them to exercise control to limit access to their information.

We agree with the principles set forth in the comments of Consumer Action. Consumers need protections that include:

- Simple, clear disclosures of how consumers' personal financial information would be used and shared, and whom it would be shared with.
- Access to and use of consumers' financial data should be limited to the express purpose for which it is being used (i.e. to pay bills or to offer financial advice) unless a consumer specifically authorizes an additional purpose.
- Data storage must be limited to the need to save individuals' data to provide an ongoing aggregation service. Otherwise providers must be required to delete consumer data as soon as it is no longer needed for the chosen purpose.
- Plain-language statements by data aggregators that they will use data provided by consumers only to fulfill customers' financial goals and that customers retain full control over data access and the ability to revoke that access.

5. Consumers should be able to access and store their data in order to move their accounts.

Consumers may wish to access their account data not only for add-on services used in connection with their accounts but also for purposes of closing the account and transferring it elsewhere. Setting up bill payments for a variety of other accounts, redirecting preauthorized charges, and even collecting and storing transaction information can be a cumbersome process. The control that financial institutions have over account data, and the difficulty of moving it elsewhere, inhibits competition and locks consumers into accounts with which they are unhappy.

The CFPB should promote an easy-to-use mechanism for consumers to export their data, close the account, and transfer the data to a new account.

6. The CFPB should supervise the larger data aggregators and intermediaries.

The complex security and privacy issues involved in the sharing of financial account data demand oversight. No federal regulator presently examines data aggregators and the intermediaries that access sensitive data. The CFPB should initiate a rulemaking to define the larger participants in the data aggregation market and begin supervising them.

7. Section 1033 should also be used to give consumers a right to access the actual consumer report or risk score used to assess the consumer.

Section 1033 of the Dodd-Frank Act provides consumers the right to access 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." 12 U.S.C. § 5533. We urge the Bureau to use this authority to give consumers the right to – or encouraging covered entities to provide access to – a copy of the consumer report or risk score that a covered person used in connection with providing the consumer a financial product or service.

We recognize that consumers are entitled a consumer report in some cases, such as after an adverse action. 15 U.S.C. § 1681j(b). However, they must seek the consumer report from a consumer reporting agency (CRA), which may provide a very different report than the report provided to the user. In the worst case scenario, the user report can reflect serious errors (such as mixed files, i.e. files that mix the information of two different consumers) that do not appear on the report provided to the consumer.

As for risk scores, while the Fair Credit Reporting Act mandates disclosure of a credit score used by the user if there is an adverse action or risk-based pricing, this disclosure is limited to scores used to "predict the likelihood of certain credit behaviors, including default." 15 U.S.C. § 1681g(f)(2)(A)(i). The disclosure does not apply to other types of risk scores derived from consumer reports and used for consumer financial services or products, such as those used for debt collection activities or for opening deposit accounts. We urge the Bureau to consider using Section 1033, or to otherwise encourage covered persons, to provide to consumers with access to other risk scores used for financial products and services.

* * *

Thank you for the opportunity to submit these comments and for your work to enhance consumers' ability to safely and easily access and use their financial account data. If you have questions, please contact Lauren Saunders at lsaunders@nclc.org, (202) 595-7845.

Respectfully submitted,

National Consumers Law Center
(on behalf of its low income clients)