

February 12, 2020

Kathy Kraninger
Director
Consumer Financial Protection Bureau
1700 G St. N.W.
Washington, D.C. 20552

Re: Consumer Financial Protection Bureau's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act

Dear Director Kraninger,

The Financial Health Network is submitting this written statement in response to your invitation to serve as a panelist at the Consumer Financial Protection Bureau's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act. We believe that clarity on this issue is sorely needed, welcome the Symposium's discussion, and encourage the CFPB to refocus on the uncertainty surrounding consumer data access.

The Financial Health Network is the leading authority on financial health. We are a trusted resource for business leaders, policymakers, and innovators united in a mission to improve the financial health of their customers, employees, and communities. Through research, advisory services, measurement tools, and opportunities for cross-sector collaboration, we advance awareness, understanding, and proven best practices in support of improved financial health for all.

Our unique position allows us to identify pain points and opportunities from both industry and consumer perspectives. Consequently, we envision a competitive, fair, and robust financial services marketplace, in which consumers' diverse transaction, savings, and credit needs are met by a range of providers offering convenient, transparent, and high-quality products and services at competitive prices.

Given our vantage point and vision for the future, the Financial Health Network has taken a particular interest in the evolution of the financial data ecosystem. Today, consumers' experience with the financial services industry is determined by providers' use of data. Broadening data availability has increased competition by lowering barriers to entry, allowed financial institutions to design better products and services, and given consumers a holistic view of their financial lives that enables them to spend, save, borrow, and plan responsibly. However, it has also presented risks of discrimination, compromised privacy, and enabled revenue models that use consumers' data in ways that they neither understand nor benefit from. This dichotomy is not unique to the financial data ecosystem, as consumers are subject to data practices they don't understand, benefit from, or have control over in every aspect of their lives. However, what is unique in the financial data ecosystem is that while larger efforts to address this challenge have stalled in Congress, the CFPB already has authority to take steps to make consumers' data work for them.

The Financial Health Network encourages the CFPB to use its authority to affirm consumers' right to access their financial data and protect consumers from emergent risks. We also encourage the CFPB to coordinate with

other regulators to ensure appropriate supervision of data aggregators, and strongly consider whether direct supervision might be appropriate.

Assessing the financial data ecosystem

In October 2016, the Financial Health Network became one of the first organizations to release [*Consumer Data Sharing Principles*](#). These consumer-focused principles provided a framework for the industry to work toward a data-sharing ecosystem that is secure, inclusive, and innovative. Specifically, our principles asserted that an inclusive and secure financial data ecosystem is one in which financial institutions, data aggregators, and third-party application providers coordinate to provide data to consumers that are:

- ***Available***: Consumers have the ability to view their financial information within the trusted and secure third-party application of their choice (“Availability”).
- ***Reliable***: Consumer financial data are timely, consistent, accurate and complete (“Reliability”).
- ***User-permissioned***: Consumers provide explicit consent for access to and use of their data. Consumers can easily view, modify and revoke consent for data sharing (“Consent”).
- ***Secure***: All entities follow applicable laws and industry best practices with regard to data privacy and security (“Security”).
- ***Limited to the application functionality***: Only the minimum amount of data required for application functionality are collected, and the data are stored for the minimum amount of time needed (“Minimization”).

These principles have stood the test of time and, along with the principles the CFPB subsequently issued in 2017, provide a useful benchmark to assess the state of the financial data ecosystem. While progress has been made in some areas, a great deal of work remains to be done to align that ecosystem with these principles. Below, we discuss each principle its own right, and comment upon the ecosystem’s progress in achieving it.

Availability

Broadly speaking, financial data are available for consumers in the United States to use within the third-party application of their choice. This is due in part to efforts by banks and data aggregators to work together to make consumers’ data available, and in part to some data aggregators’ use of “screen scraping” to allow for connectivity in the absence of Application Program Interfaces (APIs) or bilateral contracts. While measuring connectivity is difficult, some aggregators claim to cover 95 percent of US deposit accounts, and screen scraping has enabled consumers from even small institutions to connect without needing an API. However, it is worth noting that data holders’ incentives are not necessarily aligned with the principle of availability, and that unreasonably restricting data fields or charging fees for data access could threaten the progress that has been made.

Reliability

While the evolution of the financial data ecosystem has largely succeeded in making financial data available, reliability remains a point of concern. Persistent disputes between banks and data aggregators have resulted in

banks cutting off access altogether in some cases, resulting in service interruptions to consumers using third party applications. Further, the widespread use of screen scraping in our system is widely acknowledged to be sub-optimal for the purposes of timeliness, consistency, accuracy, and completeness.

Consent

Consumers provide consent for aggregators to access and use their data, but it is questionable whether they have any understanding of its implications. Moreover, the absence of meaningful ways to view, modify, or revoke consent is problematic, and limits consumers' ability to control their data. Consumers' ability to understand the terms of their consent is particularly hampered by some data aggregators' practice of using banks' branding to make it appear as if the consumer is on their bank's website. This practice should be discontinued, and aggregators hoping to build consumers' trust should work to ensure that consumer consent is knowingly given to them. That said, the Financial Health Network is heartened to see efforts by some aggregators and banks to create consumer-facing permissions dashboards. These are promising developments that may accord consumers meaningful and continuing control of their data.

Security

While the financial data ecosystem in the United States demonstrates that data sharing solutions can develop in the absence of regulation or industry alignment, this ad hoc approach has come at the expense of data privacy and security. The security challenges brought about by screen scraping are well known, and have recently been cited by the Financial Crimes Enforcement Network (FinCEN) as an emerging source of fraud. Data aggregators largely acknowledge the shortcomings of screen scraping in the long run, but point out that regulatory uncertainty and disagreements with banks over the scope of data access make it difficult to move beyond screen scraping at present. Efforts among industry-led stakeholder consortia to move away from screen scraping are welcome, but thus far have been subject to varying levels of buy-in, limited uptake of technical standards, and a perception of bias towards large, incumbent financial institutions.

Minimization

It is difficult to measure the financial data ecosystem's progress on minimization, but reports indicate that coming to a consensus on best practices will be challenging without involvement from regulators. On the one hand, there is considerable evidence that some aggregators pull data in greater amounts and with greater frequency than is required by the particular applications for which consumers give their consent. Some aggregators have even been accused of continuing to pull data from consumers' accounts after they have terminated the third-party app for which they permissioned access. These practices are troubling, and almost certainly out of step with consumers' understanding and preferences. On the other hand, accusations that some banks are unreasonably restricting the data fields for which consumers can permission access are equally troubling, and would seem to reflect anticompetitive behavior at odds with consumers' right to access.

Mitigating regulatory uncertainty

While market participants bear responsibility for some of the shortcomings of today's financial data ecosystem, the Financial Health Network believes that regulatory clarity would have a galvanizing effect on the industry to redouble its efforts. This section will briefly discuss persistent points of regulatory uncertainty within the CFPB's authority, and how the CFPB might address them.

Clarifying access under Section 1033 of the Dodd-Frank Act

As the financial data ecosystem has grown, the debate over the meaning of Section 1033 has grown with it. Is Section 1033 self-effectuating, or does consumers' right to access only take effect upon rulemaking by the CFPB? In either case, who is required to comply with this obligation, and what constitutes compliance?

In our 2017 response to the CFPB's Request for Information, we urged the CFPB to lay these questions to rest by providing principles-based guidance to affirm consumers' right to access. We stated then that such guidance from the Bureau might be the necessary catalyst to bring all stakeholders to the table to develop effective industry-wide solutions. Today, there is an emerging consensus that the Bureau's non-binding principles were not sufficient to elicit this response, and that more decisive action is needed.

In that context, we believe that undertaking a formal rulemaking process would provide a forum for stakeholder engagement while affirming consumers' right to access and providing clarity on the meaning of Section 1033 once and for all. Further, we believe that rulemaking could help to provide clarity on questions that industry has been unable to answer on its own, such as what data fields must be made available at the direction of the consumer.

Clarifying the applicability of the Fair Credit Reporting Act (FCRA)

The question of whether the FCRA applies to data aggregators divides the aggregator community and may have important implications for banks and other data sources. Do aggregators function as credit reporting agencies when supplying data at a consumer's request for use in eligibility decisions? If so, do banks function as furnishers? Most importantly, how can accuracy be assured if consumers do not have the rights and protections afforded by the FCRA?

Absent protections under the FCRA, consumers have limited visibility into and ability to correct the data transmitted by an aggregator. As data aggregators become more important to the financial data ecosystem, clarity over whether consumers have these protections is increasingly urgent. The Financial Health Network believes that the CFPB should issue guidance on the applicability of FCRA, and carefully consider how to achieve the FCRA's critical objectives if it does not apply.

Clarifying liability under Regulation E

How to clarify liability for unauthorized transactions resulting from credentials shared with data aggregators is perhaps the thorniest question facing the financial data ecosystem. Are consumers liable for unauthorized

transactions due to a data breach at an aggregator or misconduct by an employee of an aggregator? If not, is it right for banks to be held liable even if they were not responsible for the breach or misconduct? Are aggregators or third-party application providers in a position to bear the liability themselves?

In our 2017 report, [*Liability, Transparency and Consumer Control in Data Sharing: A Call to Action for Financial Services Providers and Regulators*](#), we recommended that industry create an agreed-upon liability framework for data sharing, and that regulators clarify liability under Regulation E in order to enable such a framework. We continue to believe that greater clarity is needed, and recommend that the CFPB issue guidance that consumers are not liable for unauthorized transactions originated with login credentials a consumer has shared with a data aggregator. Such guidance may help to motivate industry to come to an agreed-upon framework. In order to ensure that a future breach does not jeopardize the solvency of data aggregators or third-party application providers, we believe that the CFPB should also encourage appropriate risk mitigation policies, including third-party liability insurance.

Clarifying supervision of data aggregators

As aggregators' role in the financial data ecosystem has grown, questions as to how they should be regulated have become more pressing. Most notably, there is a lack of clarity over when aggregators are subject to oversight as third-party service providers. Differing definitions from the CFPB, FDIC, Federal Reserve Board, and OCC contribute to this uncertainty, as does the varying nature of relationships among banks, non-bank financial service providers, and data aggregators.

Given this complexity, the Financial Health Network encourages the CFPB to work with other regulators to issue interagency guidance that clarifies when aggregators are subject to oversight as third-party service providers. Further, the CFPB should strongly consider whether bringing aggregators under direct supervision via larger participant rulemaking would be appropriate in the context of other guidance.

Long term priorities

While the Financial Health Network believes regulatory clarity is necessary for building an inclusive and secure financial data ecosystem, it is not sufficient. Over the long term, the Financial Health Network believes the CFPB and other regulators should look for ways to play a more active role on two key issues.

First, a concerted effort is needed to migrate the ecosystem away from screen scraping. As discussed above, screen scraping leads to a number of sub-optimal outcomes for consumers, aggregators, third party application providers, and banks that are inconsistent with our data-sharing principles. However, screen scraping is so deeply embedded in the financial data ecosystem in the United States that stakeholders will need to take care that their efforts to phase it out do not cause unnecessary collateral damage. We believe that the steps toward regulatory clarity outlined above are necessary conditions for the ecosystem to move beyond screen scraping, and should nudge industry to make progress on that goal. However, we also believe that the CFPB must remain engaged on this challenge for years to come in order to ensure that a move away from screen scraping does not undermine consumers' right to access.

Second, the ability of small financial institutions to make consumers' data available is largely dependent on their core technology providers, particularly if the ecosystem moves away from screen scraping. Ensuring that these providers make sustainable data sharing solutions available to their customers is critical to ensuring that a meaningful right to access under Section 1033 does not exclude customers of small community banks and credit unions.

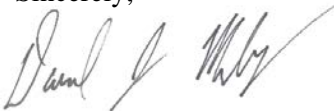
Conclusion

The Financial Health Network believes that the CFPB has a unique opportunity to take steps to ensure that consumers' right to access fosters competition, innovation, and a data-sharing ecosystem that both benefits and protects consumers. Given the seemingly incessant stories of misconduct with consumer data across industries, the CFPB's opportunity to proactively address these pressing issues in the financial data ecosystem should not be taken for granted. We believe that affirming consumers' right to access will help them to achieve financial health by increasing competition and incenting market actors to use data to design products and services that facilitate consumers financial lives.

We also believe that these actions are only the first step, and that a broader effort to assess consumers' data rights and protections in financial services is needed. The Financial Health Network looks forward to contributing to this important work, and stands ready to engage with regulators, industry stakeholders, consumer advocates, and others who believe in the importance of an inclusive and secure financial data ecosystem.

We thank the CFPB for the opportunity to share our views, and look forward to working with the agency as it considers its options.

Sincerely,



Dan Murphy
Policy Manager
Financial Health Network