3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

February 21, 2017

Ms. Monica Jackson
Office of the Executive Secretary
Consumer Financial Protection Bureau
1700 G Street, N.W.
Washington, D.C. 20552

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

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), the only national trade association focusing exclusively on federal issues affecting the nation's federally-insured credit unions, I would like to share with you NAFCU's thoughts on the Consumer Financial Protection Bureau's (CFPB) request for information (RFI), titled "Consumer Access to Financial Records."

NAFCU represents over 800 of the nation's federally-insured credit unions, all of which strive to provide their members with the products and services they need to achieve their individual financial goals. As member-owned, not-for-profit cooperatives operated by volunteer boards, credit unions have traditionally offered services that promote smart budgeting and financial planning. For example, many credit unions have helped members develop personalized budgets with the help of automated tools and savings rewards programs. NAFCU believes that the development of better personal finance products can be achieved with responsible access to consumer data. Yet such innovation must be fair and safe for the consumer.

Services fueled by customer data can drive growth in the financial sector; however, the CFPB should temper its enthusiasm for fintech innovations. The CFPB's paramount concern should not be evangelizing new financial management software, but ensuring that the costs associated with data aggregation are not foisted upon financial institutions to the detriment of consumers.

General Comments

NAFCU is supportive of the CFPB's efforts to promote consumer access to new technologies and financial services through the cultivation of an innovative and competitive marketplace. However, NAFCU does not think that financial aggregators and so-called fintechs should be able to take advantage of their special status to shift the burdens of data collection onto account providers like credit unions.

Section 1033 of the *Dodd-Frank Wall Street Reform and Consumer Protection Act* (the Dodd-Frank Act) provides that consumers are generally entitled to information about their usage of financial products or services, including transactional data. Section 1033 does not expressly state whether consumers can authorize third parties to access data on their behalf; however, the CFPB should construe the scope of sharable data narrowly in order to protect consumers from inadvertent disclosure of sensitive information. The Bureau should also recognize that information "usable by the consumer"—as characterized by the Act—may be significantly more limited than information that would be profitable for data aggregators. NAFCU advises the Bureau to distinguish between data that is necessary to deliver consumer services versus data that merely supplements the business activities of third parties.

NAFCU is aware that many financial institutions have forged beneficial partnerships with data aggregators and fully supports efforts to streamline regulatory approval of formal information sharing agreements. However, NAFCU believes that the CFPB's invocation of its Section 1033 authority may signal its intention to enforce an information sharing regime that is not governed by contracts. In the absence of clear agreements specifying terms and conditions governing information use, ad-hoc access to consumer accounts by external parties may compromise credit union services and data security. As CFPB Director Cordray has already acknowledged, not all financial aggregators are created equal[1]—and the risk of unscrupulous actors disguising harmful practices under the mantle of innovation must be taken seriously.[2]

Data security burdens should fall on the record-seeking party.

NAFCU believes that companies that request access to consumer financial records should bear the burden of ensuring that the transfer and retention of such information is secure and conforms to consumer expectations of privacy. Accordingly, NAFCU asks that the Bureau develop a robust set of data security principles for record-seeking entities which would serve as a prerequisite for access to consumer data. Such an alignment of cybersecurity responsibilities will help credit unions and other financial institutions offset the costs of an otherwise expensive vetting process for aggregators and other companies who intend to extract consumer financial data.

Enforceable standards would also serve a more critical function: protecting consumers from data aggregators who are not subject to the same rigorous privacy and data protection rules that apply to credit unions under the *Graham-Leach Bliley Act* (GLBA).[3] Many fintech companies and aggregators have touted bank-like security, but the CFPB's first data security consent order was issued in response to the deceptive cybersecurity representations of an e-commerce payment processor.[4]

---

[1] See Prepared Remarks of CFPB Director Richard Cordray at the Field Hearing on Consumer Access to Financial Records, Field Hearing on Consumer Access to Financial Records (November 17, 2016).
[2] *See* Tim Dalgeish, "Credential Sharking: A New Fraud Comes to Town," RSA Blog (April 4, 2016), available at http://blogs.rsa.com/credential-sharking-new-fraud-comes-town/
[3] See 12 C.F.R. Part 748.
[4] See Consent Order, In re Dwolla, Inc., Docket No. 2016-CFPB-0007 (March, 2, 2016).

Although NAFCU does not think that Section 1033 of the Dodd-Frank Act grants third parties any right to unfettered access to consumer information, the CFPB should nonetheless ensure that there are appropriate data security standards in place to account for situations where the financial institution and the record-seeking party have no contractual relationship specifying roles and responsibilities for safeguarding consumer information. Furthermore, an unexpected and widespread breach of multiple data aggregators might compromise the safety and soundness of the financial system, leaving credit unions and other financial institutions on the hook for resulting damages.

Lastly, NAFCU believes that the frequency of data requests issued by record-seeking companies should be regulated to the extent that they impose a burden on credit union systems. Credit unions should not pay to serve data requests to numerous companies seeking access to consumer financial records as doing so might impair the functionality of online services or necessitate costly upgrades.

Credit unions should be exempt from any Bureau-developed standard for electronic data formats.

Section 1033(d) grants the CFPB limited authority to promulgate standardized formats for transaction information made available to consumers. In NAFCU's view, the CFPB's authority is limited because Section 1033(d) narrowly contemplates standards that would meet the test of *consumer* usability described in Section 1033(a). However, the business of data aggregation frequently involves actors who are not consumers and whose data formatting needs likely extend far beyond what the ordinary consumer requires in order to use their transaction data.

NAFCU believes that the CFPB should avoid conflating the needs of consumers with the needs of third party companies who may act as agents. Although the Dodd-Frank Act does not define the term "consumer," other regulations have defined it as referring only to natural persons. See, e.g., Regulation E, 12 C.F.R. 1005.2(e). Accordingly, electronic standards promulgated under § 1033(d) should be designed to reflect consumer needs as opposed to the demands of the fintech industry. However, NAFCU believes that credit unions already provide their members with important transaction data in usable formats.

The CFPB should be aware that requiring credit unions to develop new, structured data formats would siphon resources away from member services in order to subsidize the operations of record-seeking companies. When implementing new data sharing protocols, credit unions must frequently coordinate changes with software vendors, institute new data security policies, review contracts, and invest in new hardware or software capabilities. Additional expenses would accrue if the CFPB ultimately decides to encourage industry use of structured data feeds or a standard application program interface (API). All of these costs would negatively impact the availability of credit union member services in exchange for the promise of vaguely defined innovation.

Accordingly, NAFCU believes that the CFPB should exercise its authority under Section 1022 of the Dodd-Frank to exempt credit unions from any formatting standard promulgated under Section 1033(d). Aggregators are already capable of collecting information through screen scraping techniques which a consumer can facilitate by provisioning the right credentials. The

potential development of structured data formats through a future regulatory framework would only impose unnecessary costs.

Customer control of third-party access must be a prerequisite for data sharing.

NAFCU believes that companies that have obtained permission to access consumer financial records must provide the customer with an easy method of restricting or modifying access. To adequately protect individual transaction information, consumers should have the ability to immediately withdraw permissions granting access to their records. Additionally, aggregators seeking to obtain data from account providers must offer tools that allow consumers to determine how additional parties will access their data, either downstream or upstream. These controls are essential for consumers to make informed decisions about how they want their transaction information distributed among companies that are generally not subject to the data protection standards under the GBLA.

Consumers should also have the ability to tailor permissions in a way that matches their individual risk appetite for potential fraud or abuse. Many fintech companies desiring consumer transaction information are non-bank entities not subject to examination or supervision by a traditional bank regulator. With less formal supervision, these companies are less accountable to their customers. Consumers therefore deserve tools that enable quick and easy withdrawal of data access permissions. NAFCU believes that it is incumbent upon companies seeking consumer financial records to develop and maintain these tools.

Information relating to any transaction should be construed narrowly.

Section 1033(b) enumerates various exceptions to the general rule that obligates financial account providers to supply consumers with basic transaction information in an electronic form. NAFCU believes that in order to create a secure information sharing environment, these exceptions must be interpreted broadly to ensure that consumers are not forfeiting rights to more information than is necessary to deliver the services they seek. A broad class of exemptions would also mitigate the reputational and monetary damage that would occur in the event that a data aggregator suffers a catastrophic data security breach.

The CFPB must consult with NCUA before issuing any proposal governing access to consumer financial records.

Before enacting any rule governing consumer access to financial records, Section 1033(e) requires the Bureau to consult with the federal banking agencies and the Federal Trade Commission to "take into account conditions under which covered persons do business both in the United States and in other countries." NAFCU urges the Bureau to consult with the National Credit Union Administration (NCUA) to assess how implementation of data formatting and provisioning requirements will impact the availability of credit union services and the security of member transaction data.

Credit unions owe their members a duty to safeguard and protect their sensitive financial information—a duty that may be compromised by allowing financial data aggregators to obtain and transmit transaction information among any number of downstream entities. NAFCU

believes that NCUA can offer the CFPB valuable information regarding the risks associated with potential misuse of customer data by third parties.

Conclusion

NAFCU appreciates the CFPB's efforts to empower consumers and ease market barriers so that financial data can be used in productive ways. NAFCU believes that structured data sharing can be beneficial when credit unions and third parties voluntarily contract to provide innovative services to consumers. However, the CFPB should not seek to compel unfettered information sharing, nor should it help companies offset operational, security and regulatory costs by shifting burdens onto account-providing institutions like credit unions.

Any regulatory framework that requires credit unions to build, maintain and secure structured data streams to support the operations of data aggregators would unfairly compromise credit union service and leave members more vulnerable to potential fraud. NAFCU believes that the CFPB should ensure that access to consumer financial records is predicated upon a fair distribution of costs and data security responsibilities, which should be born primarily by record-seeking parties. In any future rulemaking related to this request for information, the CFPB should also seek to exercise its Section 1022 authority to exempt credit unions from rules promulgated under Section 1033(d) of the Dodd-Frank Act. Such an exemption will ensure that credit unions can tailor their data sharing protocols in a manner that best serves their members' interests.

NAFCU appreciates the chance to submit comments in response to the CFPB's RFI on access to consumer financial records. Should you have any questions or concerns, please do not hesitate to contact me at amorris@nafcu.org or (703) 842-2266.

Sincerely,

Andrew Morris

Regulatory Affairs Counsel