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

July 14, 2023

Comment Intake
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

RE: Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information
(Docket No. CFPB-2023-0020)

Dear Sir or Madam:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing in response to the request for information (RFI) published by the Consumer Financial Protection Bureau (CFPB or Bureau) regarding data brokers and their business practices. NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve 135 million consumers with personal and small business financial service products. Attention to potential supervisory gaps among data aggregators, brokers, and other entities engaged in the collection and sale of consumer financial information is commendable and necessary to ensure a level playing field exists within the financial services industry. However, the CFPB's application of the Fair Credit Reporting Act (FCRA) to specific types of information collection should neither impair credit unions' access to data which is necessary to remain competitive, nor increase regulatory burdens for institutions already subject to the Gramm-Leach-Blilely Act (GLBA), the FCRA, and the Bureau's regulations.

General Comments

Credit unions directly and indirectly rely on data brokers to obtain information about members or prospective members. Often access to consumer data is necessary to better understand discrete market segments and provide competitive financial products and services. For advertising purposes, a credit union may provide a company with a list of home addresses in a market that overlaps with the credit union's field of membership. The company will then use that information to deliver targeted web advertisements. This exchange of information is a necessary component of scoping marketing to areas the credit union actually serves and is not a sale of information.

The information provided by data brokers also enables the use of alternative data for assessing the credit risk of consumers who lack a traditional credit score. Alternative data generally consists of non-traditional indicators of borrower creditworthiness and offers an avenue for improving

access to credit for credit invisible consumers, who represent approximately 26 million people in the United States, according to the CFPB.[1] For NAFCU members that use non-traditional data, most use it in tandem with traditional credit reports when determining creditworthiness. Many use alternative data when determining pricing for products. In 2019, 48 percent of NAFCU-surveyed credit unions reported that they utilized at least some form of alternative data for credit underwriting purposes. The type of alternative data varied by respondent, but some items included rent, utilities and telecom payment histories—information that is often collected by and purchased from data brokers.

Credit unions may also benefit from the data provided by data brokers when using software to detect fraudulent transactions and verify identity. Internally, credit unions may leverage data provided by data brokers to conduct background checks of employees. However, the use of alternative data or other data-enriched technology does not necessarily mean the credit union has a direct relationship with a data broker. In most cases, the collection of data to improve accuracy or reliability in software is managed and performed by third parties that serve as vendors or service providers. As a result, many credit unions will indirectly depend on data brokers to the extent that software used for credit scoring, underwriting or other purposes depends upon accurate and current information.

When exchanging information with affiliates and third parties, credit unions are bound to the legal requirements of the GLBA and Regulation P governing privacy of consumer information. Regulation P prohibits credit unions from sharing a member's nonpublic personal information with third parties unless an exception applies or the credit union has provided the member with a privacy notice and the opportunity to opt out of the sharing. Some credit unions are subject to state specific data privacy rules. In general, credit unions have demonstrated a strong commitment to member privacy and this conduct has helped promote the industry's good reputation as safe, dependable, and trustworthy.

However, improper data practices at insufficiently regulated businesses, including social media companies and uninsured financial technology companies, present data privacy risks that may cause Americans and their credit unions significant harm. Data breaches cost the U.S. economy billions in losses each year. However, the current patchwork of state and federal data privacy legislation and regulation is both insufficient to adequately protect any American's data across the entire economy and unnecessarily burdensome to credit unions and other federally insured financial institutions.

Need for data security standards

Congress and regulators must ensure that when fintech companies interact and compete with regulated financial institutions, they do so on a level playing field. Although the business models

[1] CFPB, A report on the Bureau's Building a Bridge to Credit Visibility Symposium (July 19, 2019), available at https://www.consumerfinance.gov/about-us/blog/report-credit-visibility-symposium/.

of data brokers remain largely distinct from those of insured depository institutions, emerging strategies that leverage new regulatory privileges—such as those under section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act)—could make data broker activities more integral to overall competition within the financial sector.[2] Companies that specialize in data aggregation can be an attractive target for cyber criminals and lack of federal data security standards for these entities can magnify the risk of social engineering attacks for consumers. Weaknesses in data broker security can also increase credit unions' exposure to fraud.

While depository institutions have for decades complied with a national standard on data security since the passage of the GLBA, the same cannot be said for entities that are neither subject to the federal banking regulators Safeguards Guidelines or the FTC's Safeguard's Rule. Some companies that might be considered data brokers could potentially operate outside of both frameworks if their collection and sale of data is nonfinancial in nature. However, nonfinancial data can be enriched for financial purposes and data brokers may be service providers to financial companies otherwise subject to the FTC's Safeguard's Rule.

Although the FTC requires covered financial institutions under its jurisdiction to ensure that service providers have adopted data security safeguards by contract, the FTC does not have the same supervisory reach as the federal banking agencies and does not have the ability to review these contracts outside of enforcement actions. Accordingly, data brokers remain subject to very little federal data security oversight despite the significant role they play within the broader financial sector.

The CFPB has recognized that even among nonbanks that are already subject to the FTC's rule, there may be a need—especially in the data aggregation space—to impose more specific data security standards.[3] NAFCU recommends the CFPB take further action in this area and ensure that nonbanks handling consumer financial data are held to the same strong standards as credit unions under the GLBA.

Implementation of Section 1033 of the Dodd-Frank Act must account for gaps in data aggregator supervision

As the CFPB proceeds with development of a proposed rule to implement section 1033 of the Dodd-Frank Act, it should ensure that entities that fit the RFI's definition of a "data broker" are subject to appropriate oversight when they are acting as "authorized third parties" as that term is defined in the Bureau's Outline of Proposals on Personal Financial Data Rights. Appropriate

[2] *See* CFPB, Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Required Rulemaking on Personal Financial Data Rights, 3 (March 30, 2023) ("Data access rights also hold the potential to intensify competition in consumer finance.").
[3] *See id*. at 11.

oversight should account for both compliance with future data security standards as well as the FCRA, if applicable.

NAFCU recommends the Bureau clarify in a future proposal what types of data aggregation activities might make a third party a credit reporting agency under the FCRA and Regulation V. If some data aggregators and other recipients of consumer data are not regarded as credit reporting agencies, then the Bureau should clarify what rights consumers may exercise to dispute inaccuracies or errors introduced by these entities. However, the Bureau should not adopt a framework where an authorized third party may redirect disputes regarding data accuracy to a data provider instead of performing its own reasonable investigation of an alleged error.

Another action the Bureau can take to improve oversight of data aggregators is to exercise its larger participants authority as requested in a joint letter submitted by NAFCU and other trade associations.[4] Regardless of how the Bureau chooses to implement section 1033, it should fill supervisory gaps that might grant data aggregators preferential treatment and exacerbate consumer privacy risks if left unaddressed. At a minimum, the Bureau should reexamine the scope of its larger participants rule for the consumer reporting market if it has already recognized that "data users may compete for customers with the data holders from which they have obtained data."[5]

The CFPB should not pursue policies that impair financial institution access to data markets or introduce additional regulatory burdens for credit unions.

The RFI asks whether companies using new business models are covered by the FCRA, given the FCRA's broad definitions of "consumer report" and "consumer reporting agency." As noted above, additional clarity would be helpful in terms of understanding what data broker activities would result in the generation of a consumer report. However, the CFPB must be cautious about overextending FCRA restrictions to certain types of information in a way that frustrates credit unions' ability to conveniently and affordably access data that is necessary to remain competitive and protect members.

Subjecting identifying information (i.e., "credit header data) not traditionally regarded as a component of creditworthiness to FCRA permissible purpose restrictions would have adverse effects on a credit union's ability to protect its members against fraud or identity theft. Credit header" information includes identifying information such as name, address, date of birth, and Social Security number. Such information may be obtained from a credit report "header" and

[4] *See* Letter to the Honorable Rohit Chopra, Director, Consumer Financial Protection Bureau, re: Petition for rulemaking defining larger participants of the aggregation services market (August 2, 2022), available at https://www.nafcu.org/joint-petition-cfpb-larger-participant-rulemaking-data-aggregation-services-File 30
[5] *See* CFPB, Consumer Access to Financial Records, 85 Fed. Reg. 71003, 71006 (Nov. 6, 2020), available at https://www.federalregister.gov/documents/2020/11/06/2020-23723/consumer-accessto-financial-records. 4 See Taskforce Report

from other reports that only contain identifying information. If such information were subject to permissible purpose restrictions, credit unions might encounter difficulty in obtaining certain reports, incur additional compliance costs with respect to the information that is obtained, and face potentially greater litigation risk. These factors could degrade credit unions' efforts to confirm identities and prevent financial crime. Accordingly, the CFPB should not take any action to designate credit header information as part of a consumer report.

The CFPB should also seek to preserve and promote financial institution access to both traditional and nontraditional data without inviting additional abuse of the dispute process under the FCRA. NAFCU has heard of dispute tactics aimed at overwhelming the administrative resources of a financial institution in the hope that it forgets or is unable to respond in time. Unfortunately, there is no limit on how many times a member can dispute a credit report online. Many "credit fixing companies" merely send form letters and consumers are provided with an unrealistic assessment of their odds of success. These companies are not in any way helping the member which is unfortunate because members pay money for their services.[6] As such, should the CFPB move forward with actions related to clarifying the scope of the FCRA to data broker activity, it would be helpful to also address industry concern regarding excessive disputes.

Credit invisible populations are best served when markets for consumer data operate competitively. Imposing new regulatory restrictions on the use of alternative data or information exchange with data brokers would limit credit unions' ability to compete and market effectively. Policy actions aimed at regulating the use alternative data would also deprive consumers of a healthy market for affordable credit and could potentially exacerbate the already strained conditions of the credit dispute system.

Conclusion

NAFCU appreciates the opportunity to respond to this request for information. NAFCU supports efforts to close regulatory gaps that might otherwise increase the risk that nonbank companies will cause consumer harm. Credit unions are committed to using consumer data responsibly and safely to provide affordable financial products and services to millions of Americans. The CFPB should prioritize efforts to promulgate data security standards for data brokers and ensure appropriate supervision of larger participants in the data aggregation markets.

At the same time, the CFPB should avoid policy actions that would impair credit unions access to data that is needed to remain competitive or introduce new and costly compliance burdens for institutions already subject to the GLBA, FCRA and their implementing regulations.

If we can answer any questions or provide you with additional information, please do not hesitate to contact me at 703-842-2266 or amorris@nafcu.org.

[6] https://www.nafcu.org/newsroom/nafcu-trades-flag-credit-repair-scams-lawmakers

Sincerely,

Andrew Morris
Senior Counsel for Research and Policy