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 4, 2021

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

RE: **Consumer Access to Financial Records; RIN: 3170-AA78**

Dear Sir or Madam:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing to share our comments regarding the Bureau of Consumer Financial Protection's (CFPB or Bureau) advanced notice of proposed rulemaking (ANPR) related to implementation of section 1033 of the *Dodd-Frank Wall Street Reform and Consumer Protection Act* (Dodd-Frank Act). NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 123 million consumers with personal and small business financial service products. NAFCU believes that development of innovative personal finance products can be achieved with responsible access to consumer data. However, such innovation must be fair and safe for the consumer and the credit union. Accordingly, the Bureau should avoid implementing section 1033 in a way that impairs a credit union's ability to protect its members' data from the risk of theft or abuse.

General Comments

Financial data aggregation generally refers to the collection of consumer information across different accounts at different institutions or companies, a service often performed by, but not limited to, third parties. In general, there are two primary methods for aggregating consumer data: accessing account information directly through application programming interfaces (APIs), which provide a standard specification for structured data exchange, or through screen scraping, which often involves a machine accessing an account as if it were a human user.

Screen scraping is less favored among financial institutions because sharing user login and password information with a third party introduces significant security concerns. NAFCU's September 2018 Economic & CU Monitor Survey found that approximately 20 percent of credit union respondents were using APIs for data sharing purposes while 80 percent did not currently share data on member transactions with third parties. While the share of credit unions using APIs for data sharing has grown since 2018, sharing *member data* with third parties does not appear to have become as commonplace.

As the ANPR acknowledges, the market for data aggregation services can be characterized as one where data aggregators perform services for data users (i.e., third party service providers), but

recent trends suggest that data aggregators are increasingly performing the functions of service providers. In recognition of the blurred distinction between aggregators and data users, NAFCU's comments are framed primarily in terms of the distinct roles of traditional financial institutions (often the data holders) and their fintech counterparts (often aggregators or data users).

In general, section 1033 aims to provide a formal mechanism for making consumer data portable. While data portability can serve as the foundation for more streamlined integration of financial technology, faster account opening, and automation of credit decisioning processes, it can also lead to greater security risks, particularly when consumers are not able to provide informed consent to third parties seeking data access privileges. Currently, credit unions that do provide structured account or transaction data to aggregators or fintech partners are free to negotiate the terms of such access by contract. The bilateral formation of a contractual agreement helps ensure that any data seeking party meets minimum security and privacy standards, and that the terms of the data sharing agreement are fair to the credit union and its members. Such contracts may even identify specific technical standards (e.g., transmission encryption, storage encryption, adherence to ISO specifications), and help allocate legal liabilities to different parties in the event of a security incident.

NAFCU recognizes that some forms of data sharing can occur without strict privity of contract between data exchanging parties. If consumers want to share the data contained in electronic bank statements, for example, they are free to do so, and NAFCU supports consumers having a right to access such records. In fact, credit unions would likely face competitive disadvantages if consumer-managed data sharing required formal agreements between data holding institutions and data users or aggregators. To require a contract in every instance would magnify the bargaining power of larger technology companies and could force smaller credit unions to accept unfavorable terms and conditions regarding data rights in order to provide members with access to popular services. For example, a smaller credit union might find it difficult to support their members' use of a large technology company's account management or bill pay software if adequate data retention or destruction provisions were absent in a standard form contract.

To best accommodate both modes of data exchange (company-to-company versus entirely consumer managed), NAFCU recommends the Bureau seek to preserve credit unions' ability to define the scope of third-party data privileges, as well as channels for data sharing that exist outside of formal contacts. At the same time, the Bureau should explore the value of minimum data and privacy safeguards for non-supervised entities that seek to acquire consumer information without relying upon agreements with data holding institutions.

Interpreting section 1033 to supersede formal data sharing arrangements risks impairing the benefits of credit union due diligence, particularly if the Bureau intends to recognize a third party's right to request and access data on consumers' behalf.[1] If section 1033 accords such broad data privileges, credit unions would no longer be able to exercise discretion and judgment when defining the scope or terms data access; instead, they might be expected to accommodate virtually

[1] The ANPR contemplates third-party access privileges insofar as it defines "authorized data access" as third-party access to consumer financial data pursuant to the relevant consumer's authorization.

any request from a data user or aggregator regarding access to "information relating to any transaction, series of transactions, or to the account including costs, charges and usage data." At the same time, consumers would assume greater responsibility for managing their own data privacy and security when interacting with third parties. To the extent consumers are unable to accurately judge the security of data seeking entities, failure to limit data access could erode the overall resilience of the financial sector and expose consumers to greater risk of fraud. NAFCU believes that the significant data security and privacy risks associated with section 1033 warrant a limited interpretation of its data portability framework that preserves credit unions' ability to define the terms and scope of permissioned data access.

Given the complexity of defining a regulatory framework for data sharing that accommodates the differing priorities of credit unions, fintechs, and large banks, while simultaneously protecting consumers from potentially greater security and privacy risks, NAFCU does not believe that the Bureau should pursue an expansive rulemaking to implement section 1033. More specifically, NAFCU asks that the Bureau avoid developing any future rule that would impinge upon credit unions' freedom to define the scope of data sharing arrangements to best serve their members.

Granting third parties expansive data privileges could impose unreasonable costs on credit unions that lack the scale and sophistication to accommodate section 1033's open-door conceptualization of data access rights. In addition to absorbing the costs of developing or acquiring the necessary IT infrastructure to support such a regime, implementation of section 1033 would make it harder for credit unions to protect their members' data from misuse. Lastly, limited fields of membership could dilute the benefits which might exist for credit unions in a section 1033 rulemaking while rewarding fintech companies disproportionally—particularly where there is disregard for the value of traditional financial institutions' custodial functions.

Benefits and costs of consumer data access

The Bureau observes in the ANPR that "the number and usage of products and services that utilize or rely upon consumers' ability to authorize third-party access to consumer data have grown substantially and rapidly." Some of this growth corresponds with distinct use cases, such as personal financial management tools, financial advisory services, and assistance in shopping for and selecting new financial products and services. The ANPR further notes that authorized data access holds the potential to intensify competition and innovation in many, perhaps even most, consumer financial markets.

While analytic capabilities have long been a component of credit unions' strategic toolset, the proliferation of large and well-maintained databases of transactional information has made it easier to draw insights about member financial behavior, automate underwriting, and optimize delivery channels for financial advice, such as through consolidation of account information. NAFCU surveys suggest that a significant share of credit unions are already utilizing member data to better understand cash flow patterns, improve collateral management, and tailor advertisements based on location and transactional histories. In a January 2021 NAFCU survey, 21 percent of credit union respondents indicated that section 1033 could make it easier for their members to use popular

fintech applications. At the same time, an ever larger share of respondents predicted that section 1033 would make it harder to protect member data.

For consumers, the primary "cost" of section 1033 implementation will be heightened exposure to data security risks and loss of privacy. An extreme interpretation of section 1033 could make it difficult for a financial institution to prevent a third party known to have substandard cyber hygiene from acquiring data if the consumer has provided their permission. From the consumer's vantage, a third party's lack of appropriate safeguards may not be fully known until after the fact if data seeking entities are not subject to regular examinations like traditional financial institutions and data holding financial institutions cannot employ guardrails through contractual provisions.

Consumers might also grant greater data rights than are necessary to derive useful functionality from a third-party financial application or service. The likelihood that consumers will face actual harm related to the security and privacy of their data will depend on whether the Bureau requires non-supervised third parties to meet minimum security and disclosure requirements before exercising section 1033 privileges to obtain financial records from data holders.

Competitive incentives and authorized data access

It is likely that any future decision to implement section 1033 will alter the competitive landscape for credit unions. NAFCU anticipates that a formal set of rules governing financial data access rights will confer the greatest benefit upon entities that are able to serve any consumer from any location, which could have the effect of amplifying the limitations of credit unions. Since the passage of the Dodd-Frank Act, the number of credit unions has declined by over 30 percent. This may be attributed to a combination of regulatory stresses, low interest rates, competitive pressures from larger banking entities, and more recently, digital advantages possessed by fintech companies. Implementation of section 1033 could have the effect of accelerating consolidation within the credit union industry and reduce access to financial services in underserved or rural communities.

Enhanced data access privileges for third parties will likely enhance the viability of busines models that leverage wholly digital platforms. Financial companies that operate entirely online, for example, could obtain insights about consumers' financial behaviors without ever needing to be physically present in the communities they wish to serve. Although this model of banking is becoming more commonplace, mass aggregation of consumer data coupled with the ability to render real-time credit decisions (and counteroffers) could have the effect of commoditizing the market for financial products and services in way that makes it impossible for smaller credit institutions to compete against larger, more sophisticated entities. The displacement of credit unions in the long run could potentially reduce access to affordable credit in communities that have faced historical disenfranchisement. Additionally, the loss of traditional, brick and mortar institutions could exacerbate the digital divide that often exists in underserved and rural communities.[2]

[2] Pew Research Center, "Digital gap between rural and nonrural America persists," (May 31, 2019), available at https://www.pewresearch.org/fact-tank/2019/05/31/digital-gap-between-rural-and-nonrural-america-persists/.

Research published by the Federal Reserve has found that "[physical] branches continue to be an important banking channel for consumers, especially for deposit and withdrawal transactions and for resolving problems."[3] The same research found that both urban and rural counties lost 7 percent of branches between 2012 and 2017. Data through 2019 show that trends identified in the Federal Reserve's study have, if anything, accelerated on the banking side. Where that study showed that 7 percent of bank branches were lost between the years 2012 and 2017, that number has grown to 11 percent through 2019. By contrast, from 2012 through 2019, credit unions added offices to their branch network. While the additions were modest, with a net gain of 1 percent, they at least demonstrate credit unions' ongoing commitment to maintaining a physical presence in their communities at a time when many companies see value in shifting operations online.

Implementation of section 1033 could accelerate a general decline in branches by magnifying the competitive dynamics that are driving disaggregation of banking services and growth of purely digital financial services. While NAFCU supports efforts to eliminate barriers to online customer acquisition and service, such as by reforms to rules governing electronic signatures, implementation of section 1033 could effectuate a far more radical shift in how banking services are provided, in ways that could potentially devalue the relationship-banking model.

Credit unions may derive benefits from standardized data access rules, such as a more options for members to consolidate account information spread across multiple institutions and greater confidence that fintech companies that connect with their members are held to minimum data privacy and security standards. Credit unions may also be able to draw insights about their members' existing financial habits to tailor products or services more efficiently. However, potential enhancements to marketing efforts could be tempered by the reality of limited fields of membership, and it is arguably the marketing value of section 1033 data that will exert the greatest competitive influence. Unlike fintech companies that operate nationally, most credit unions would find it challenging to leverage data acquisition privileges with the same ease as, for example, a company that can invite anyone to share their financial data in exchange for a promotional rate.

The marketing value of data collected by credit unions would be discounted to the extent it concerns consumers outside the credit union's field of membership. Credit unions already face unique barriers in terms of marketing efficiency (paying comparatively more for advertising when placements fall outside the boundaries of the credit union's membership) and section 1033 could amplify those disadvantages; credit unions would be compelled to offer their data freely but would not be capable of taking full advantage of a data rich environment.

Implementation of section 1033 could also compromise credit unions' ability to guard trade secrets insofar as broad access to transactional data might permit third parties to reverse engineer credit decisioning algorithms or variables. Credit unions devote a significant share of their budgets towards developing analytical tools to derive proprietary insights about financial patterns that can

[3] Board of Governors of the Federal Reserve System, "Perspectives from Main Street: Bank Branch Access in Rural Communities" (2019), available at https://www.federalreserve.gov/publications/november-2019-bank-branch-access-in-rural-communities.htm.

inform development of new products or services. Sometimes these insights are critical to allowing the credit union to compete against other financial companies possessing greater economies of scale. The importance of developing analytical tools and platforms cannot be overstated. Over 94 percent of respondents surveyed in NAFCU's 2020 Report on Credit Unions indicated that information technology was an area that will drive spending over the next three years, and most respondents indicated that within this domain, most investments would flow towards data analytics and marketing. Implementation of section 1033 could undercut the value of these investments and hobble smaller credit unions that already face significant structural limitations.

Data security

By far the most significant concern for credit unions regarding implementation of section 1033 relates to the security of their members' information. Credit unions are held to stricter standards under the *Gramm-Leach Bliley Act* (GLBA) than companies who are not directly supervised by federal banking agencies. This is partly due to the fact that the Federal Financial Institutions Examination Council (FFIEC) has promulgated far more specific standards and guidance to implement the GLBA's safeguards provisions, and also because FFIEC agencies—including the National Credit Union Administration (NCUA)—have developed specialized procedures for assessing the security posture of regulated institutions. Credit unions receive regular cybersecurity focused examinations, whereas this may not be the case for every third-party data aggregator or data user.

NAFCU does not support an interpretation of section 1033 that limits credit unions' freedom to define data sharing terms; however, should the Bureau choose to recognize a broad right to access data on behalf of consumer, it must limit the applicability of this right to financial institutions covered by the GLBA and subject to Regulation P. In the absence of a national federal data security standard and national data privacy standards, granting entities who are not subject to these laws and regulations broad data access privileges would be irresponsible. Furthermore, the Bureau's lack of regulatory authority in the domain of data security (i.e., the Safeguards portion of the GLBA) will tend to frustrate efforts to develop common standards for non-supervised entities without significant reliance on the Federal Trade Commission, which itself lacks the supervisory toolset that would be necessary to address section 1033's security-related risks.

A section 1033 rule that permits liberal third-party access privileges could also devalue the stewardship of consumer data held by credit unions if parties that request access to credit union data are not expected to make comparable investments in security. Additionally, third party data users might engage in arbitrage strategies by relying on traditional financial institutions as the primary repositories for customer data; for example, by pulling data only when necessary to render point-in-time decisions and using data holders as the de-facto IT hosts for personally identifiable information (PII). While this might promote, incidentally, a more secure method for processing financial data, it could also foist a greater share of data security responsibilities onto the data holder who pays for the long-term security of PII.

For credit unions, the ongoing cost of protecting members' financial data is significant since it involves not only the entire IT infrastructure which supports digital and online banking operations,

but also the specific cybersecurity costs associated with mitigating data breaches and security incidents that occur beyond the walls of regulated financial institutions. Credit unions also face examination and compliance costs related to supervision of data security. NAFCU's 2020 *Federal Reserve Meeting Survey* revealed that the share of credit union operating budgets devoted to cybersecurity has increased 225 percent since 2015.

Credit unions who have earned the trust of their members by investing in security should not be forced to jeopardize that protection and investment by accommodating the requests of parties whose security posture may be an unknown variable. Contractually defined agreements, by contrast, afford credit unions the opportunity to perform required due diligence and protect members who may lack the sophistication to judge the integrity of a particular financial application that demands data access. Some credit unions have even observed that a regulated format or method for effectuating open transfers of data could introduce security risks of a significantly greater magnitude should a criminal actor abuse the broad privileges of API-level access to member data.

Implementation of section 1033 could also make it more difficult for financial sector participants to understand where data security responsibilities begin and end. In the absence of defined liability and indemnity provisions, allocating the costs of events like data breaches would be difficult using only the broad framework outlined in the statutory text of section 1033.

Although a clearly defined liability framework would be desirable in conjunction with any attempt to implement section 1033, it may be unworkable for the Bureau to allocate legal responsibilities efficiently between potentially numerous third parties who are downstream users of consumer data. A not unlikely scenario that might complicate such a framework could involve an aggregator that experiences a breach involving data it acquired from another aggregator, which was originally acquired from the consumer's primary financial institution. In such a scenario, the original data holding institution might suffer reputational damage, fraud losses or need to pay to reissue credit cards for affected consumers, even if it bears no responsibility for the breach. The financial institution would also need to resort to the vagaries of state law to obtain a remedy and would potentially face dilution of its claims for damages if other data users and data holders are affected. Data breach cases such as these are already difficult to resolve under current law, and it is likely that section 1033 could exacerbate their complexity.

In the absence of formal agreements, one mechanism for better allocating data security responsibilities between data holders, users, and aggregators would be a national, federal data security and privacy standard. Such a standard should harmonize existing federal data privacy laws, recognize credit unions' existing compliance with the GLBA, preempt state privacy laws, and implement proper guardrails for consumers' protection across the entire data ecosystem rather than just certain sectors.

Standard-setting

NAFCU recommends that the Bureau refrain from prescribing technical standards to enforce the use of a particular data sharing format since it is unlikely that a regulatory specification will satisfy

the unique security requirements and IT parameters of every credit union or keep pace with evolving cybersecurity risks. Whenever data is shared outside a credit union, a risk assessment is performed, and federal agencies such as the National Institute of Standards and Technology have generally recognized that there is no one-size-fits-all solution for cybersecurity. The Bureau should heed this advice and avoid promulgating a rule that could either force credit unions to compromise their cybersecurity or purchase new IT technology merely for the purpose of effectuating the free transfer of data to third parties.

The Bureau should, however, explore the value in limiting the risks associated with screen scraping and consumer-managed data sharing. This might involve identifying incentives that would help third parties navigate towards more secure data sharing methods. The Bureau might, for example, pursue development of a voluntary data format specification through a tech sprint, which could then be made freely available to parties interested in engaging in structured data sharing. For financial institutions that lack the sophistication or infrastructure to share data, the availability of technical resources would offer a more natural incentivize to accommodate enhanced data portability as opposed to strict rules.

Lastly, to the extent the Bureau seeks to accommodate third party requests to access consumer data, it should clarify that financial institutions that provide data in response to section 1033 requests are not data furnishers for purposes of the *Fair Credit Reporting Act* (FCRA) and Regulation V. Credit unions that transfer data in this way would be complying with their members' requests to share records, not furnishing such information by agreement or with any expectation that the data might be used to evaluate consumer creditworthiness. Furthermore, credit unions will likely possess no knowledge regarding a third party's intended use for data it obtains through a consumer's exercise of section 1033 rights.

Access scope

Credit unions should retain the discretion to control access to certain forms of data, such as transactional metadata and pricing information that may be sensitive to reverse engineering. As discussed previously, credit unions' ability to compete effectively depends upon their ability to derive useful insights about their members' financial habits and needs.

While section 1033 provides an exception for sharing "any confidential commercial information, including an algorithm," that does not preclude the possibility that such information could be discovered through analysis of basic transactional data. For example, a competitor might derive insights about a credit union's underwriting parameters by observing the relationship between deposit history and increases to an existing line of credit. Although NAFCU does not support granting third parties broad data access rights to transactional and account data, should the Bureau adopt such a policy, it must aim to limit data acquired through the exercise of section 1033 rights to no more than what a consumer would find on their regular bank statement.

Consumer control and privacy

Although NAFCU does not believe an expansive implementation of section 1033 is warranted, the Bureau may nonetheless conclude that promoting third party access rights is desirable. If it does, NAFCU recommends that these rights correspond with appropriate rules to protect the privacy and confidentiality of consumer financial records. Additionally, the Bureau should clarify whether there are limits to consumer consent that would have the effect of restraining downstream use of data by third parties.

Credit unions have demonstrated a long history of compliance with the privacy requirements contained in the GLBA and the Bureau's Regulation P. Additionally, the NCUA's implementation of the GLBA's safeguard requirements requires all credit unions to protect their members' data, including member data that is shared with service providers. Appendix B to 12 CFR Part 748 provides that a credit union should be able to address "incidents of unauthorized access to member information in member information systems maintained by its service providers". In practical terms, this means that a credit union's contract with a vendor should require the vendor to address incidents of unauthorized access to member information.

An expansive interpretation of section 1033 could frustrate credit unions' ability to protect the confidentiality of member data if there are no agreements or standards in place governing how a data user or aggregator will address matters of data privacy, confidentiality, or incident response. Even in cases where a contract does exist, the reality of conducting business with larger technology companies might require credit unions to weigh the benefits of providing access to a new service or product against the cost of relying upon boilerplate privacy or security assurances that cannot be negotiated. In such cases, the Bureau might explore the value of minimum data security and privacy standards for non-supervised companies that acquire data from financial institutions but have so far enjoyed fewer regulatory restraints and outsize bargaining power.

In general, when exercising section 1033 rights, consumers should know exactly what data a third party will be requesting on their behalf, for what purpose it is being used, how frequently it will be accessed, how long it will be stored, with whom it might be shared and under what conditions, and any rights they may assert in the event their data is lost or stolen. Additionally, consumers should be given control over how much data they choose to share if the entirety of their financial history is not necessary to furnish a particular service or credit decision.

Given the heightened risk of fraud in the event that consumers' financial data is compromised, the Bureau should regard these disclosures and controls as reasonable safeguards for third parties whose data requests are predicated on the rights or privileges recognized under section 1033. Consumers should also be granted the ability to easily revoke third party data access at any time by contacting the third party. The burden of revoking consent should not fall entirely upon a financial institution.

Interagency Coordination

Before issuing 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 NCUA to assess how implementation of section 1033 will impact the availability of credit union services and the security of member transaction data.

Conclusion

NAFCU supports efforts to empower consumers with modern financial tools and believes that regulatory barriers should not prevent financial data from being used in productive ways. However, the Bureau should not seek to compel unvetted information sharing that could ultimately harm consumers; nor should it tilt the playing field to benefit companies who hope to offset operational, security and privacy costs by shifting burdens onto account-providing institutions like credit unions.

Any regulatory framework that compels credit unions to build, maintain and secure structured data streams to unilaterally support the operations of aggregators and other third parties would unfairly compromise credit union service and distort the financial sector's competitive landscape. The Bureau must ensure that access to consumer financial records is predicated upon a fair distribution of costs, data security and data privacy responsibilities that does not overburden credit unions who already face competitive pressure and reduced bargaining power when interacting with larger technology companies.

NAFCU appreciates the chance to submit comments in response to the CFPB's ANPR 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
Senior Counsel for Research and Policy